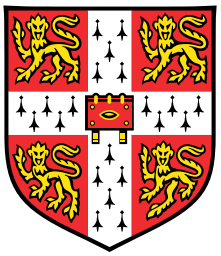
The Security of Self-Differencing Avalanche Photodiodes for Quantum Key Distribution



Alexander Mark Koehler-Sidki

Department of Engineering
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Sidney Sussex College October 2019

Thesis

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Alexander Mark Koehler-Sidki
October 2019

Abstract

The Security of Self-Differencing Avalanche Photodiodes for Quantum Key Distribution *Alexander Mark Koehler-Sidki*

Quantum key distribution (QKD) allows two users to communicate with information theoretic security by encoding information on single photons. This security is based on the laws of physics and as such can never be broken in theory. However, in practice, components do not always behave according to their theoretical models and these deviations can be exploited by an eavesdropper.

In recent years, exposing loopholes in QKD systems, known as quantum hacking, has attracted significant attention. The components most susceptible to being hacked are the single-photon detectors, often avalanche photodiodes (APDs), as they are directly exposed to the optical channel. Whilst measurement-device-independent QKD removes detector vulnerability from the system, secure key rates with this technique can be much lower than point-to-point links. As such, mitigating attacks on QKD systems is a pressing challenge in QKD.

In this thesis, the focus is on a special class of detectors, self-differencing APDs (SD-APDs), which have facilitated state-of-the art demonstrations of QKD. The susceptibility of SD-APDs to blinding attacks, the most explored and successful attack to date, was investigated and it was shown that by following best practice for their operation, such an attack would be unsuccessful. We have also proposed and developed a countermeasure such that the onus for appropriate operation could be removed from the user.

We have also explored an arguably more dangerous attack, in the form of the after-gate attack. We have shown that delayed detection events, ordinarily considered detrimental in QKD, can provide inherent protection against this attack. Finally, backflashes in GHz-gated APDs were investigated for the first time and it was shown that threat they pose to QKD security is negligible. These results highlight the inherent protection to a number of attacks that self-differencing APDs possess. We stress that the findings presented in this thesis are also applicable to other types of fast-gated InGaAs APDs that don't possess self-differencing circuitry.

Acknowledgements

There are a number of people who have made significant contributions to this work, whether in a scientific context or otherwise, and I would like to express my gratitude to them.

Andrew Shields for giving me the opportunity to carry out my research at Toshiba which has proven to be a stimulating place to work. Seb Savory for his supervision from the University of Cambridge as well as the flexibility and support he has provided on numerous occasions, without which I would have not been able to complete the PhD.

Zhiliang Yuan for his enthusiasm, support and shear breadth and depth of knowledge which never ceased to amaze me. Your attention to detail, both in the laboratory and at the desk writing papers has been vitally important.

James Dynes for his clarity of thought and logical approach to experimental problems; many issues have been fixed thanks to a quick discussion with you.

Marco Lucamarini for his patient and measured approach, particularly with regards to explaining, occasionally repeatedly, some of the more subtle theoretical points to me. Your calm and caring manner, without judgement, has provided me with a lot of confidence and encouragement and is an attitude I will seek to emulate.

Being a PhD student means being part of a community and as such I would like to pay special thanks to my fellow students. Bruno Villa for being the best cubicle mate I could have asked for and giving me a lot of support for drawing software, both technical and aesthetic; George Roberts for many useful QKD discussions and many more not useful non-QKD ones; Innocenzo De Marco for sharing the lab with me and imparting some of his LabView wizardry; Matthew Anderson for always being willing to be a sounding board to bounce ideas off, whether in a scientific framework or otherwise; Mirko Pittaluga for the many coffee breaks; Jamie Lee, Martin Felle, Christiana Varnava, Lucian Comandar, Ziheng Xiang, Mariella Minder, Christian Dangel, Jonathan Müller, Louise Wells, Raymond Smith, Ginny Shooter, Andrea Barbiero, for the many memorable lunch breaks, pub trips and cake gatherings in the kitchen.

I would like to also express my thanks to my parents, Paulette and Wolfgang, whose love and support has been unwavering and integral to who I am today and what I have achieved.

Finally, I would like to thank my wife Maddy, who has put up with the day-to-day frustrations and challenges but has never been anything other than loving and caring and always willing to listen. You have undoubtedly been the most important person to me in every respect and nothing accomplished in this thesis would be possible without you.

Publications

Parts of this thesis have been published in the following journals and talks have been given at international conferences

Journal publications

- "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution", Physical Review Applied, **9**, 044027 (2018).
  A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan and A. J. Shields.

- "Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation", Physical Review A, **98**, 022327 (2018).
  A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. L. Yuan and A. J. Shields.

- "Intrinsic Mitigation of the After-Gate Attack in Quantum Key Distribution through Fast-Gated Delayed Detection", Physical Review Applied, **12**, 024050 (2019).
  A. Koehler-Sidki, J. F. Dynes, A. Martinez, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan and A. J. Shields.

- "Backflashes in fast-gated avalanche photodiodes in quantum key distribution", In preparation.
  A. Koehler-Sidki, J. F. Dynes, T. K. Paraïso, M. Lucamarini, A. W. Sharpe, Z. L. Yuan and A. J. Shields.

Conferences

- "Setting best practice criteria for self-differencing avalanche photodiodes in quantum key distribution", Contributed talk, SPIE Security + Defense, Quantum

Information Science and Technology III, Warsaw, Poland, September 2017.
A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, S. J. Savory, Z. L. Yuan and A. J. Shields.

- "Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation", Poster, QCrypt 2018, Shanghai, China, August 2018.
A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. L. Yuan and A. J. Shields.

Table of contents

List of figures

Nomenclature

Roman Symbols

APD Avalanche Photodiode

BB84 Bennett Brassard 84

CV-QKD Continuous Variable Quantum Key Distribution

CW Continuous Wave

DFB Distributed Feedback

DOF Degree Of Freedom

DV-QKD Discrete Variable Quantum Key Distribution

ETSI European Telecommunications Standards Institute

FPGA Field-Programmable Gate Array

IM Intensity Modulator

LD Laser Diode

$LiNbO_3$ Lithium Niobate

MDI QKD Measurement Device Independent Quantum Key Distribution

PBS Polarising Beamsplitter

PNS Photon Number Splitting

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

QRNG Quantum Random Number Generator

RSA Rivest, Shamir, Adleman protocol

SD Self-Differencer

SMU Source Measure Unit

SNSPD Superconducting Nanowire Single Photon Detector

VOA Variable Optical Attenuator

WCP Weak Coherent Pulse

Chapter 1

Introduction

1.1 What is cryptography?

Secrecy underpins much of the modern world. Safeguarding sensitive information, whether bank details or medical history or missile launch codes, is of significant importance and as such has stimulated extensive work on the subject. The act of communicating this information between parties relies on a method of encrypting it such that it cannot be deciphered by any others. Broadly speaking, this is cryptography.

Cryptography as a means of communicating securely has been employed in varying degrees for thousands of years. The Spartans in ancient Greece initially practised it using a 'scytale' and Julius Caesar is said to have used a simple substitution algorithm (that now bears his name) to encode messages to his generals [2].

The underlying aim of cryptography is to determine a way of sending information which any hostile eavesdropper cannot access. In practice, forms of communication can be divided into 2 types of security:

- **Computational**: A protocol that is computationally secure is safe from an adversary about whom you have made reasonable assumptions related to their computational power. However, as the adversary improves their computer, so must you improve your protocol.

- **Information theoretic**: If a method is information theoretic secure, this means that your message cannot be decoded by an eavesdropper who does not possess knowledge of the encryption key, regardless how powerful she may be.

Information theoretic modes of cryptography do exist. Vernam's cipher [3], also known as the one-time pad, was developed and subsequently mathematically proven to be information theoretic secure by Claude Shannon [4]. However, it requires a

string for encryption and decryption, the key. This must be of equal length as the message to be sent securely between the two parties, and this key may only be used once. Furthermore, either the two parties must hold the key beforehand or must use a secure channel to distribute such a key. This means that there is no practical benefit to the protocol but it raises the theme of key distribution on which much of modern cryptography is based.

1.2 Quantum Key Distribution

Public key encryption algorithms, such as RSA [5], exist to provide a means for transmitting a key securely between two parties, without the need for them to hold any prior shared secret information. The security of this is generally based on the difficulty of factorising very large numbers, which contemporary computers struggle with. However, quantum computers are exponentially faster at solving certain problems, one of which is factorising [6]. In recent years, progress in quantum computers has accelerated dramatically [7, 8] and it is estimated they could soon overtake the most powerful 'classical' computers in the near future. Such an achievement would significantly compromise much of communication security in the modern age.

One possible, and relatively advanced, solution exists in the form of quantum key distribution (QKD). Unlike RSA, QKD schemes possess information theoretic security due to their reliance on the laws of nature or, more specifically, quantum mechanics. The simplest way to illustrate this is to consider a specific protocol of QKD, indeed the first, called BB84, named after its creators, Charles Bennett and Gilles Brassard, and the year in which it was presented, 1984 [9].

A sender, Alice, would like to transmit a secure key to a receiver, Bob. To do this securely she manipulates a specific characteristic of single photons due to their quantum mechanical nature, namely that a making a measurement causes a perturbation in the system [10]. In line with the original demonstration, let us assume she controls their polarisation. The steps she carries out are as follows:

1. **State preparation** She first chooses a basis with which to polarise her photon, usually either rectilinear or diagonal. She then chooses a bit, 1 or 0, corresponding to vertical and diagonal, and horizontal and anti-diagonal states respectively. The chosen states are nonorthogonal to one another to ensure any measurement performed by an eavesdropper, Eve, would perturb the system and thus reveal itself.

2. **Transmission** Alice sends her qubits to Bob along the quantum channel, either free-space or optical fibre.

3. **Measurement** Once the photons arrive at Bob, he chooses a polarisation basis with which to measure each particle. If he chooses the same basis as Alice, known as a compatible basis, he extracts the correct bit. Choosing an incompatible basis leaves him with a 50% probability of extracting the correct bit. He is then left with a raw key.

4. **Sifting** Bob then publicly announces over a classical channel which basis he used to measure each bit and Alice publicly informs him if he chose a compatible basis. Bits measured with incompatible bases are then discarded, leaving Bob with the sifted key.

5. **Parameter estimation** Alice and Bob then publicly compare a small subset of remaining bits to determine the quantum bit error rate (QBER). This value represents the proportion of bits that are different between Alice and Bob, even when a compatible measurement basis was used and is conservatively assumed to arise exclusively due to an eavesdropper interfering, although contributions from imperfect state preparation and detector dark counts, for example, also play a part.

6. **Error correction** Alice and Bob then perform error correction to account for the different bits between them, thus ensuring their strings are identical.

7. **Privacy amplification** Finally, Alice and Bob perform mathematical algorithms known as privacy amplification to guarantee the security of the remaining bits. Alice and Bob are then left with a shared string of bits of which Eve has no information, known as the secure key. This is outlined in Fig. 1.1.

The security of this scheme relies on two properties of quantum mechanics. Eve wishes to gain knowledge of the key by reading the information encoded on the photons and remain undetected. If she tries to perform an intercept-and-resend attack, whereby she measures the polarisation directly, she cannot know if she has chosen a compatible basis with Alice. Therefore, if she tries to send her own photon onto Bob with the same state in order to preserve her secrecy, half the time she will send the incorrect state. Since Bob measures the correct state with an incompatible basis half the time as well, the legitimate users will extract a QBER of 25% and detect Eve's presence. It is also not possible for Eve to make a copy of the transmitted photon for later measurement due to the no-cloning theorem [11].

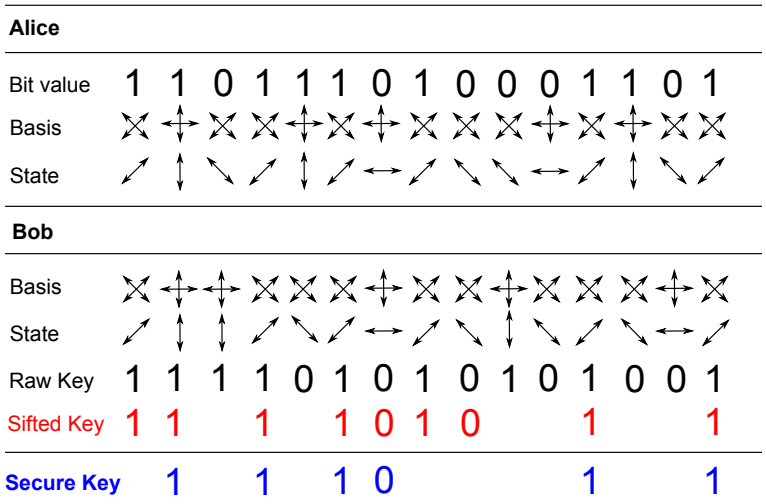


Fig. 1.1 **BB84** *An example of the BB84 protocol*

1.3 QKD protocols

The above description of BB84 is an example of discrete variable QKD (DV QKD) and is the most mature technique for performing QKD (an outline of the first demonstration performed in 1989 can be found at [12]) and also the current state-of-the-art [13, 14]. DV-QKD utilises single photons for encoding and therefore single photon detectors are employed at Bob's end, however there are several specific protocols used in this way. For example, Section 1.2 outlined a polarisation encoding scheme for BB84. Whilst this works well over free-space, where polarisation states can travel with relatively small perturbation, this technique is less suited to use over fibre. Therefore, phase-encoded schemes are often used, which involve Alice encoding her qubits in the phase difference between pulses pairs which are then decoded at Bob using a Mach-Zehnder interferometer.

For simplicity, we will focus on BB84 for the remainder of the introduction. Other protocols, such as differential phase shift and coherent one way, are introduced later in section 2.5.

1.4 QKD security

Each QKD protocol uses a particular quantum mechanical property with which to encode information, whether that be polarisation [15, 16], time-bin [17, 18], phase [19], distributed phase [20] or even the differential quadratures of phase [21–23]. Often, different protocols are suited to different scenarios, determined by the simplicity of the protocol or suitability for integration into a network configuration. Another major

consideration is the level of security they provide, or rather the class of attacks against which they are secure against [24]:

- **Individual attacks.** As the name suggests, this addresses schemes whereby Eve interacts *individually* with each qubit and she also uses the same strategy throughout.
- **Collective attacks.** As above but she is able to store her ancillas in a quantum memory for later measurement (say after Bob publicly announces his basis choice).
- **Coherent or general attacks.** Eve can perform any attack allowed by the laws of quantum mechanics.

Although QKD can be shown to be information theoretic secure in theory, in practice this may not be true, largely due to deviations of components from their ideal behaviour. These imperfections can provide side-channels for Eve to exploit, meaning that QKD systems require continuous characterisation and testing, eventually resulting in hardware or software modifications or incorporating these deviations into security proofs.

As example, in an ideal case, Alice would utilise a perfect single photon source with which to encode her key. Currently, single-photon sources have been unable to reach the brightness suitable for practical QKD [25], therefore heavily attenuated laser pulses (with average photon numbers less than 1), known as weak coherent pulses (WCP), are used to simulate single photons. However, due to the coherent nature of WCPs, the output is a Poissonian distribution [26] meaning there is a finite possibility of an output pulse containing more than one photon [1].

Eve could then employ a photon-number-splitting attack (PNS) [28, 29] whereby she siphons off any additional photons and stores them in her quantum memory before performing her measurement after Alice and Bob publicly exchange basis information. This loophole was then closed with the advent of the decoy state method [30, 31], whereby Alice sends a range of fluxes to Bob, which usually consist of a signal, decoy and vacuum pulse [19]. By analysing the photon statistics at Bob for each state, the users can determine whether Eve is attempting to mount a PNS attack. This problem has also been tackled separately with the implementation of the SARG04 QKD protocol [32], but this has largely been abandoned in favour of the decoy state method as it scales less favourably with distance [24].

[1] Even if the non-attenuated source is not necessarily Poissonian and demonstrates, say, Bose-Einstein distribution, the statistics after the attenuator can be well approximated as Poissonian [27].

A further prominent example is the Trojan Horse attack, whereby Eve again aims to target imperfections at Alice's side. Eve injects strong light into the transmitter's setup which undergoes the same phase modulation used for encoding single photons for key distribution. By measuring the reflection, Eve can learn which states Alice chooses and thus obtain the key [10, 33], shown in Fig. 1.2. By considering a practical setup, a quantitative security analysis was performed resulting in a passive countermeasure that can be used with reasonably high confidence, in this case an isolator at Alice [34].

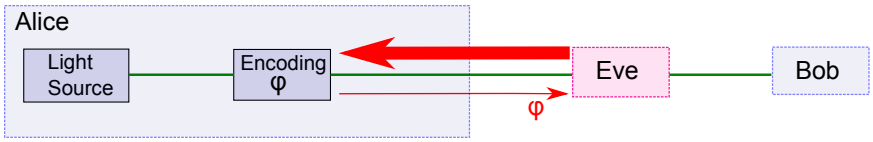


Fig. 1.2 **Trojan horse attack** *Eve injects strong light into Alice's system and measures the reflection from her encoding device and can thereby extract the bit encoded by Alice.*

1.4.1 Measurement device independent QKD

Due to the vulnerability of detectors within a QKD system (see Chapter 2 for examples), protocols have been explored that are detector side-channel free [35, 36]. Due to its ability to be implemented with current technology, significant work has focused on measurement-device-independent QKD, or MDI-QKD. This protocol utilises a third, untrusted party, conventionally known as Charlie, who carries out any detection and publicly broadcasts his results. Briefly, Alice and Bob each have a source of photons on which they encode one of the BB84 polarization states. They then each send their photon to Charlie who carries out a Bell State Measurement, BSM, on both particles by means of 3 sets of beamsplitters and recording any coincidence counts (see figure 1.3). This type of measurement relies on the Hong-Ou-Mandel (HOM) effect [37] which states that indistinguishable particles incident on the same input port of a balanced beamsplitter will leave from the same output port. After announcing his results, Alice and Bob publicly disclose their chosen bases (but not states) and are left with a perfectly anti-correlated string of bits. Bob then flips the necessary bits and him and Alice now share a secure key [38]. In contrast to other QKD protocols whereby Alice has a key she wishes to send to Bob, here neither Alice nor Bob start out with a complete key; it is only through each of them encoding information on their photons and by listening to Charlie's measurement results that they obtain a key. As such, were Charlie to be replaced with Eve, she would gain no information as to the key by controlling the detectors.

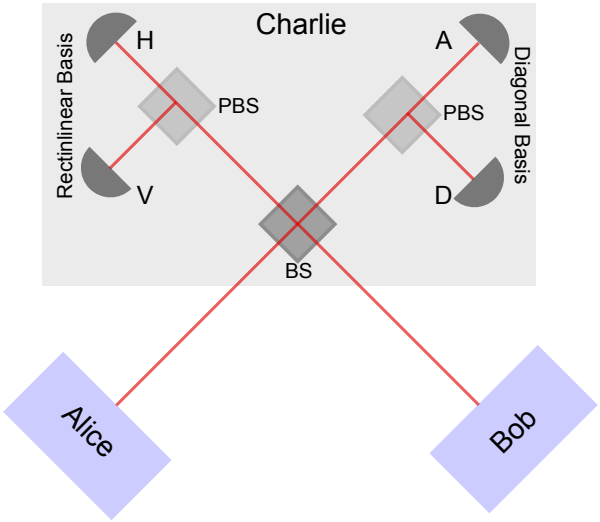


Fig. 1.3 **Basic principle of MDI-QKD** *All detection is carried out at an untrusted node, Charlie, hence detector side-channels are removed.*

One recent study on MDI-QKD was carried out in [39] using optically seeded lasers, whereby a master laser was used to inject a slave laser. This allowed for high visibilities and consequently coincidence counts, allowing for much higher secure key rates than the highest previously achieved [40]. However it is important to note that this work was only a proof-of-principle experiment as it did not employ real-time polarisation basis or state modulation. Although MDI-QKD removes the existence of detector side-channels, it is likely unsuitable for widespread adoption due to the difficulty of performing two-photon interference, even with the laser-seeing technique demonstrated in [39]. Furthermore, over medium distances, the secure key rates are significantly lower than point-to-point links (ref).

Since MDI-QKD relies on the existence of coincidence counts, which only arise due to very precise photon arrival times, the key rates can still be low when compared to two-party QKD schemes. As such, detector-device-independent QKD (DDI-QKD) was developed [41]. In this method, a photon is sent by Alice and encoded in one polarisation degree of freedom, DoF, and then sent to Bob, who then encodes another DoF on the same photon before performing a BSM, on this particle. After announcing the result of the BSM, Alice and Bob can obtain a secure key. In this way, Alice and Bob are not reliant on coincidence counts at Charlie's detectors for obtaining their key and can therefore obtain much higher key rates than with MDI-QKD. Once more, however, the most recent experimental implementation was also proof-of-principle [42]. Furthermore, unlike MDI, in order for the security to be guaranteed, Eve cannot have direct access to the detectors used for the BSM [42–44].

A recently proposed protocol, known as Twin-Field QKD (TF QKD) [45] appears to provide the detector side-channel free characteristics of MDI-QKD in addition to extending the achievable distance such that it overcomes the fundamentally unsurpassable bound [46]. The increased performance arises from it using the interference of optical fields, rather than individual photons. This has stimulated a significant body of work, with several proof-of-principle implementations taking place [47–50], as well as additional variants such as sending-not-sending [51, 52] and security analyses [53].

1.5 Practical QKD

When considering real-world implementation, QKD performance and security is subject to a number of caveats. These arise due to practical constraints on what is available to Alice and Bob. For example, in theory, Alice and Bob will use an infinitely long key for the purpose of encoding their secure message. Of course this is impossible as the users have limited computational power, hence they have to take into account the finite length of the key when carrying out error correction and privacy amplification so as to have an accurate estimate of Eve's knowledge of the key [54]. This procedure naturally impacts the secure key rate, giving a more pessimistic estimate. The analysis of the two cases are generally referred to as the asymptotic and finite-key size analyses.

The secure key rate is dependent on a number of system parameters, some of which are due to physical properties of components, others to protocol choice or security analysis technique.

QKD is generally performed either over free-space or fibre (although recent underwater implementations have also taken place [55–57]). Whilst free-space demonstrations have shown promise in recent years, most notably in the performance of the Micius quantum satellite [58–60], fibre-based systems are the most promising future candidates for widespread implementation. This is largely due to the stability offered by installed fibre and also the existence of mature fibre infrastructure. As such, the channel loss is well defined, typically at 0.2 dB/km for currently installed fibre [61] or 0.16 dB/km for ultralow-loss fibre [14]. In addition to this, crosstalk from classical traffic can also play a part, but for simplicity we assume dark fibre is used.

The performance of the detectors at Bob, or indeed Charlie, have arguably the most direct impact on the secure key rate. The detection efficiency naturally allows a higher proportion of sent qubits to be correctly measured. However, a trade-off often arises between the efficiency and detector dark count rate, a characteristic which limits the achievable distance of QKD. This occurs because the losses become much

larger at longer distances, thus degrading Alice's transmitted photons and reducing the signal-to-noise ratio.

The proportion of detected bits to sifted bits is determined by the choice of protocol. For standard BB84, since each basis has an equal probability of being chosen, the sifting efficiency is 50%. This can be improved using alternative protocols; for example in the T12 protocol it is very close to unity [19].

The sifting efficiency can be improved further by expanding the choice of protocols outside of those similar to BB84. The distributed phase shift protocol only employs one basis, therefore Alice and Bob always have compatibly bases and the sifting efficiency is unity. The drawback of this protocol is its security has not yet been proven against coherent attacks.

The overall operating frequency of the system also directly affects the key rate. This feature is limited by the bandwidths of the sources at Alice and the detectors at Bob/Charlie, with the state-of-the-art systems employing 1 or 2 GHz-clocked systems [13].

We can analyse the impact of these parameters on the secure key rate. Usually, weak coherent pulses combined with decoy states are considered but for simplicity we will examine the relationship between the key rate and distance by assuming a perfect single-photon source where there is no need for decoy states and the raw key is infinitely long. We start with the probability of a detection or click at Bob's detectors, given by equation 1.1:

$$P_{click} = \eta_{chan} \times \eta_{det} \tag{1.1}$$

where η_{chan} is the channel loss and is given by $10^{-\frac{\alpha L}{10}}$, where α is the loss coefficient in fibre ($0.2\ dB/km$) and L is the distance in km. η_{det} is simply the detection efficiency of Bob's detectors, which we assume to be 30%. We then define the quantum bit error rate (QBER), which is in its simplest form the probability that, given a click, there will be an error. These errors are conservatively assigned to the presence of an eavesdropper, however, in practice, imperfections in the QKD system have a significant impact. For example, if Alice and Bob have poor interferometers with low visibility, this increases the probability of incorrect bits being measured, even if compatible bases between the legitimate users are chosen. Furthermore, if Bob uses detectors with a high dark count rate, the probability of multiple detectors clicking in a system is higher. In this case, Bob randomly chooses a bit, which thereby increases the number of errors. The QBER is defined in equation 1.2:

$$e = \frac{P_{err}}{P_{click}} = \frac{1}{2}\frac{P_{dark}(1-P_{click})}{P_{click}+P_{dark}} + \frac{1}{2}P_{ap} + P_{opt}. \tag{1.2}$$

The denominator in the first term indicates the total number of clicks. The numerator is then the probability of an incorrect bit being measured even when a compatible basis is chosen. This arises when the correct detector does not click, $1-P_{click}$ but the incorrect one does, due to a dark count, P_{dark}. The afterpulsing probability, P_{ap} is then treated separately as these clicks are uncorrelated with Alice's qubits, therefore have a probability of $\frac{1}{2}$ of generating an error. P_{opt} is the error due to optical misalignment, possibly as a result of poor interferometers discussed earlier. For the purpose of determining the key rate, we take values of P_{dark} to be 10^{-6}, P_{ap} to be 3% and P_{opt} to be 1%. The secure key rate is then given in equation 1.3:

$$R \geq qP_{click}\{1-h(e)-fh(e)\} \tag{1.3}$$

where q is the basis choice probability, which is 0.5 for BB84, $h(x)$ is the binary Shannon entropy and is given by $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ and f is the error correction efficiency, which is simply taken to be 1.15. Using the aforementioned parameters, we plot the secure key rate as a function of distance as the black line in Fig. 1.4. We see that using low loss-fibre (0.16 dB/km), detectors with a higher dark count rate (10^{-4}), efficient BB84 protocol, such as T12 [19] ($q = \frac{15}{16}$) or incorporating a detection mismatch or blinding parameter (multiplying $1-h(e)$ by a coefficient of 0.79 [62]) all have a significant impact on the secure key rate.

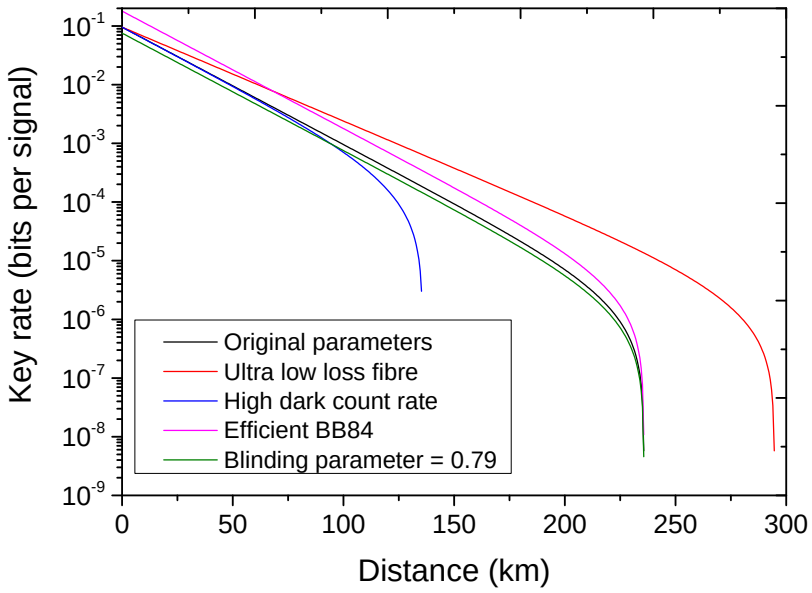


Fig. 1.4 **Key rate comparison** *Secure key rate in bits per signal as a function of distance in km. This shows the effect that various parameters can have on the key rate, such as using ultra-low loss fibre, a more efficient protocol or by incorporating a blinding parameter.*

1.6 Current implementations of QKD

Since its initial conception, QKD has developed considerably, such that it is on the cusp of becoming a part of everyday life. However, implementation techniques still differ widely, meaning it is useful to survey the range of methods and components used for carrying out QKD.

1.6.1 Channel

When considering the quantum channel over which QKD performed, this can essentially be divided into either free-space or fibre implementations.

The first experimental demonstration of QKD was performed over 30.5 cm of free space [12] and since then it has developed significantly, culminating in the demonstration of satellite to ground QKD in [60]. Whilst this was a landmark achievement where QKD was performed over extraordinary distances, free-space QKD faces hard challenges in the forms of atmospheric turbulence and beam wandering which can degrade the QKD signal. On the other hand, it benefits from the ability to exploit visible wavelengths for transmitting qubits, for which high-performing detectors are readily available.

The latter is the more mature technique, largely because the fibre infrastructure required is already in place but also because the loss is easy to characterise, usually at a rate of 0.2 dB/km. This also makes the implementation of a quantum network more straightforward than over free-space and has spurned the development of several networks [63–65]. In all likelihood, both techniques will combined, much as they are with current classical transmission which employs both wired and wireless transmission, in order to maximise coverage.

1.6.2 Sources

As discussed in section 1.4, in an ideal world, QKD would be performed with single-photon sources. However, the current state-of-the-art is insufficiently bright for practical QKD. As such, distributed feedback (DFB) laser diodes attenuated to very low light levels such that they emit weak coherent pulses (WCPs) are more commonly used.

WCPs display a Poissonian distribution, where the probability of emitting an n-photon state is given by the following equation:

$$P(n) = \frac{\mu}{n!} e^{-\mu} \tag{1.4}$$

where μ is the average number of photons. Due to the aforementioned photon number splitting attack, average fluxes are usually less than 1 in order to minimise the number of multi-photon components. By employing the decoy state method, QKD using sources of this type are still secure. Although systems employing true single-photon sources can offer potentially higher secure key rates [66, 67], the availability and ease-of-use of laser diodes means it is unlikely they will be supplanted in the near future.

1.6.3 Detectors

The choice of detector has a significant impact on the key rate both as a result of its detection efficiency and dark count rate. Furthermore, it is the most vulnerable component in the QKD system due to its exposure to the optical channel. As the detectors are the focus of this thesis, it is useful to survey in detail the current state-of-the-art, which is summarised in Table 1.1.

For fibre-based systems, InGaAs avalanche photodiodes (APDs) have developed to become the prime candidate for single-photon detectors at Bob. This is largely due to their (close to) room-temperature operation, very good single-photon detection characteristics, reasonably low-cost and low footprint. Within that category, different modes of operation have evolved, with the vast majority of systems and groups using gated detectors due to their capability for large count rates. To further increase the count rates, several background cancellation techniques have been developed, namely sine-wave gating, dummy mode cancellation and self-differencing, the latter of which has resulted in record detection efficiencies of 55% [68].

The other major alternative to APDs are superconducting nanowire single-photon detectors (SSPDs). As the name suggests, these consist of nanowires that are cooled to superconducting levels which are then biased close to their critical current, which is the point at which the wire becomes resistive. When a photon impinges on the nanowire, a local hotspot is created where the temperature is raised and the resistance changes, thus triggering a voltage pulse which can be measured. These can offer detection efficiencies that easily exceed 80% as well as dark count rates as low as 0.1 mHz [69]. However, the need to operate them cryogenically, usually at 2K or lower, which means they are also bulky makes them unlikely to be widely adopted, although they could be suitable for specific high-value applications.

Detector	T (K)	η (%)	DCR (Hz)	Jitter (ps)	Max CR (MHz)
Passive APD [70]	163	10	1	400	0.05
Sine wave APD [71]	243	30	2000	138	10
SD APD [68]	243	55	30000	91	500
SSPD [69]	1.6	67	0.0001	29	2000
SSPD [72]	0.8	93	1	150	25
TES [73]	0.2	98	-	-	-

Table 1.1 **State-of-the-art single photon detectors** *for fibre-based QKD. T: temperature; η: single photon detection efficiency; DCR: dark count rate; CR: count rate; SD APD: self-differencing avalanche photodiode; SSPD: superconducting nanowire single-photon detector; TES: transition edge sensor.*

1.6.4 State of the art QKD

The current situation of QKD is one of great promise and significant advances have taken place in recent years. As discussed, it is likely that fibre-based systems will carry out the bulk of QKD and form the backbone of any quantum networks in the future. This can be seen with the announcements of several QKD networks throughout the globe [15, 63–65]. In the context of this, there have been several landmark studies. In terms of maximum achievable distance over which keys have been distributed, the previous record of 404 km [74], which was performed using MDI QKD, has recently been overtaken; firstly, by a group using a simplified variant of BB84 and aided by ultra-low loss fibre and high efficiency SSPDs [14], next through the use of the new protocol of TF-QKD [75]. Secure key rates at shorter distances have also reached record levels thanks largely to improved data processing techniques [13].

Whilst fibre-based QKD systems have developed significantly, the loss associated with fibres combined with the lack of availability of quantum repeaters places an absolute limit of achievable distance. As such, interest grew surrounding satellite QKD, where the losses could be significantly reduced and this culminated in the demonstration of QKD using the Micius satellite [58]. It is possible that in the future, a network of satellites combined with a fibre-based network including trusted nodes will provide global quantum-secured communication.

1.7 Motivation for research

Public key encryption techniques, such as RSA, currently guarantee the security of everything from bank details to personal health records. However, they will become obsolete once quantum computers that are capable of performing Shor's algorithm with sufficiently small numbers of errors are built. With the recent announcement of quantum supremacy being (possibly) achieved [76], replacing current encryption techniques that are not susceptible to the threats of quantum computers is becoming increasingly urgent.

The security of QKD is guaranteed by the laws of physics and can therefore offer information theoretic security irrespective of the development of quantum computers. It is now rapidly approaching a level of maturity where it can be considered for commercialisation. Its potential as a cryptographic primitive has stimulated significant developments in recent years and has resulted in pilot network field trials in several continents [15, 65, 77–79]. For widespread implementation, InGaAs APDs are the most attractive candidates due to their ability to operate close to room temperature whilst displaying excellent detection characteristics and having a small footprint. Those using self-differencing circuitry demonstrated the highest count rates, largest detection efficiencies and greatest secure key rates, making them the current best-performing detectors.

As such, addressing loopholes associated with detector attacks is a pressing concern in order to maintain such a high level of security. Whilst MDI-QKD closes all detector side-channels, it is difficult to implement and offers lower key rates at short distances compared to point-to-point QKD. It is therefore desirable to improve the implementation security of more mature two-party systems.

The problem can be tackled in two ways. The first way is to devise countermeasures to these attacks, such that an eavesdropper, whose only restriction is to be bounded by the laws of physics, cannot perform said attack. Whilst attractive in theory, in practice this is a difficult objective to achieve, as it usually involves hardware modifications which either introduce additional complexity or loss. Furthermore, extra components need characterising and could contain loopholes of their own, as well as the fact that it is difficult to prove the effectiveness of a countermeasure.

The second way, which is gaining more attention, as shown by the work of ETSI (European Telecommunications Standards Institute) [80], is to define best-practice criteria and eventually standards for each component, in order to minimise Eve's capability. This requires some assumptions about Eve's capabilities and therefore aims at satisfying 'practical' security. Since many of Eve's attacks are not possible with current technology as they require significant advances, in quantum memories,

for example, it is perfectly valid to aspire to practical security. Furthermore, many experimentally demonstrated attacks rely on improper or inappropriate operation of components, making the need for universal standards even more pressing.

As mentioned, detectors are the most vulnerable components in the QKD system, hence it is natural to focus on these devices for exploring QKD security. Due to their ability to demonstrate excellent single-photon detection without the need for cryogenic cooling, APDs are the most natural choice for QKD implementation. The state-of-the-art detectors employ self-differencing circuitry for improved signal-to-noise which has enabled QKD systems using such detectors to obtain record secure key rates [13]. Therefore, improving the practical security of self-differencing avalanche photodiodes would be a significant step in guaranteeing the security of a QKD system and enabling it to be widely implemented.

1.8 Organisation of thesis

The thesis is organised to reflect the overall aim of the PhD, which was to improve the security of self-differencing APDs in QKD. Therefore, individual techniques that have been demonstrated as attacks were examined and measures to mitigate them were demonstrated. Chapter **2** gives a background to avalanche photodiodes, particularly focusing on their quenching techniques. Chapter **3** illustrates how inappropriate operation of self-differencing APDs provides a backdoor for Eve and outlines the best-practice criteria for operating these detectors to restrict Eve's hacking ability. Chapter **4** describes the implementation of an intensity modulator to act as an active measure against Eve's blinding attack. The extinction required for successful blinding prevention is characterised and a discussion surrounding its security is presented. Chapter **5** explores how the after-gate attack can be mitigated by exploiting delayed detection events, phenomena usually considered detrimental for QKD but here exploited to the users' advantage. Chapter **6** characterises backflashes in fast gated APDs and relates their effect on Eve's information to the secure key rate. Chapter **7** concludes the thesis and discusses the overall significance of the results before providing direction for future research.

Chapter 2

Background

2.1 Introduction

This chapter will provide an overview of single-photon avalanche photodiodes (APDs), including the device structure. The various techniques used to operate them, specifically with regards to quenching, will also be introduced. The literature surrounding previous attacks on detectors in QKD systems will also be explored.

2.2 Avalanche photodiodes

Avalanche photodiodes (APDs) are, broadly speaking, reverse-biased PN- or PIN-structured semiconductor devices that absorb incoming photons and generate electron-hole pairs. Most significantly, APDs contain an additional multiplication region allowing them to possess internal gain, therefore a single photon can generate enough carriers which results in a macroscopic current detectable by conventional electronics, removing the need for a separate amplifier which could introduce additional noise. This particular characteristic makes APDs very practical single-photon detectors and this, coupled with their ability to operate at temperatures reachable with thermo-electric cooling, or even room temperature, make them ideal candidates for QKD.

As discussed previously, fibre-based QKD is the most mature and attractive technique, therefore detectors need to be sensitive to light of wavelengths that propagate with minimal loss over fibre, usually at either 1310 or 1550 nm [10]. Many APDs used for these wavelengths are currently manufactured with a structure based on the separate- absorption-and-multiplication regions (SAM) design which was first proposed in [81]. The SAM heterojunction structure was developed in order to reduce the existence of dark currents that arose from tunnelling that was evident in previous

homojunction APDs [82]. The most common combination of materials for these layers are InGaAs and InP, for use as the absorption and multiplication regions respectively [83]. InAlAs [84, 85] and silicon [86] multiplication regions have also been explored due to the materials' large k-coefficients (sometimes referred to as the excess noise factor or ionisation rate ratio) which is the ratio of the electron, α , and hole, β , ionisation coefficients [87]. It has been shown that for an ideal case, this value should either equal 0 or ∞ so that only one type of carrier contributes to the avalanche process and therefore the multiplication noise is at its lowest [88]. For InP, holes have a higher coefficient [89, 90] and therefore the structure of these devices is optimised to accelerate holes, rather than electrons, to the multiplication layer. Later the SAGM or SAGCM design was developed which included grading and charge layers respectively [91]. The grading layer, usually InGaAsP for InGaAs/InP APDs, is used to increase the rate of transition of holes from the absorption to the multiplication region by grading the discontinuity in valence-band between the two layers [92, 93]. The charge, or field control, layer allows for higher flexibility in controlling the internal electric field profile [91, 94]. This is outlined in Fig. 2.1.

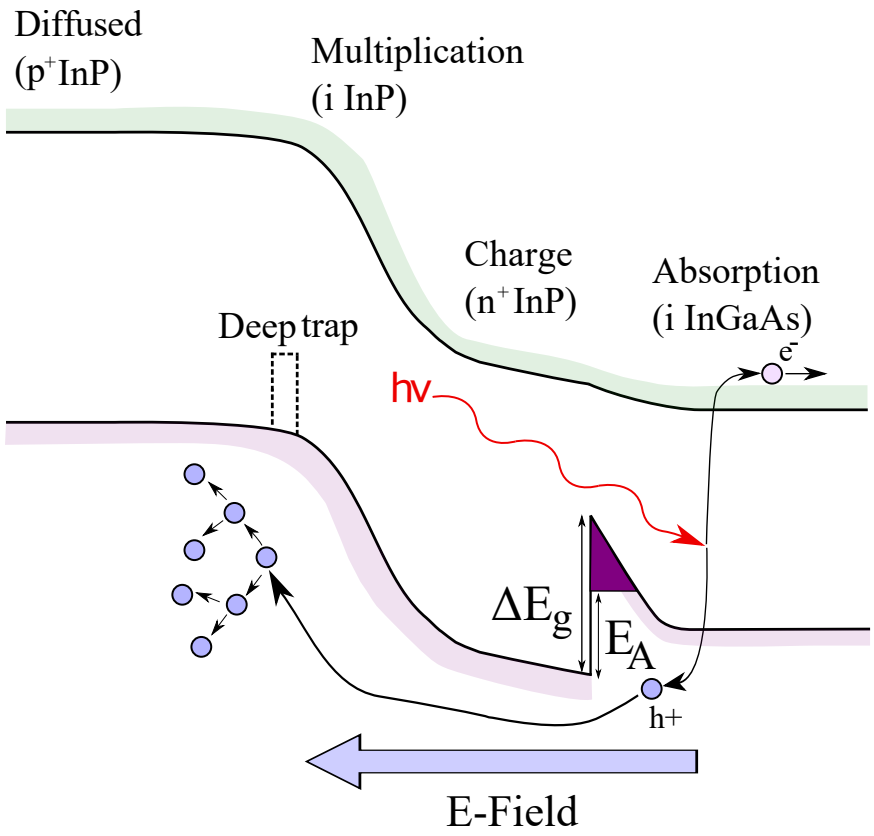


Fig. 2.1 **SAM APD** *Band diagram of the separate absorption, charge and multiplication structure of an InGaAs/InP APD, where E_g is the band gap offset and E_A is the effective barrier height.*

2.2.1 Characteristics

As mentioned earlier, APDs are attractive candidates for QKD largely due to their ability to demonstrate strong single-photon detection at temperatures reachable by thermo-electric cooling [68] or even room temperature [95]. This places them ahead of superconducting nanowire single-photon detectors (SSPDs) which have very high detection efficiencies (exceeding 85% [96]) but have to be cryogenically cooled, typically to below 2 K [97]. APDs also register high count rates due to their low dead times, again an advantage over some SSPDs [96] and transition edge sensors [98]. In this section, I will outline the characteristics of interest for single-photon APDs in QKD. For a more general review on single photon detectors, I refer the reader to [99, 100].

Detection efficiency

The most crucial characteristic when examining the merit of an APD in the context of QKD is its single photon detection efficiency (SPDE). It specifies the probability that an incident photon is detected. It is given by the following equation:

$$SPDE = P_{abs} \times P_c \times P_{av} \times P_{det} \tag{2.1}$$

where P_{abs} is the photon absorption probability, i.e. whether an incident photon generates an electron-hole pair, P_c is the probability that a carrier, either a hole or an electron depending on the device, arrives at the multiplication region, P_{av} is the probability of an avalanche taking place [101] and P_{det} is the probability of detecting an avalanche which is dependent on the external circuitry. The first two factors multiplied together give the external quantum efficiency, and is the absolute upper bound of the device's single-photon detection efficiency. Equation 2.1 gives a strong insight into how the detection efficiency of a device might be improved. For example, improving the grading between the absorption and charge regions to minimise the effect of the lattice mismatch and 'trapping' at the subsequent potential well can increase P_c or improvements in anti-reflection coatings can increase P_{abs}

Dark count rate

Dark counts arise, as the name suggests, when the detector fires without any incident light or, more specifically, when a carrier is generated by means other than photoexcitation. In general, these counts arise either due to thermal generation, which is

dependent on the band gap of the absorption material as well as the temperature [102] or various tunnelling effects, either band-to-band or trap assisted [101]. Dark counts can also arise from carriers generated in different regions of the absorption layer or even outside the active area [103].

Afterpulsing

Another contribution to APD noise arises from so-called 'afterpulsing'. These are counts that occur due to the release of carriers that were trapped in previous avalanches [1]. If such a detrapping occurs during a time interval where the APD is primed for detection (sometimes referred to as an 'ON' period), it can trigger an avalanche of its own. In order to reduce this effect, it is often desirable to reduce the 'ON' time and allow a longer dead time between detection events which creates a smaller avalanche charge per event and thus lower afterpulsing [68]. This is due to the fact that afterpulses are generally thought to arise from defects in the InP multiplication region, hence fewer charges reduces the probability of trapping [1, 104, 105]. The afterpulsing probability has been directly included in previous treatments of the QBER [106], as shown in Eq. 1.2.

This shows the afterpulsing probability can directly impact the performance of the QKD system, where if it is greater than 22%, the QBER would exceed 11% and above this threshold most protocols would abort key exchange altogether.

Dead Time

The time between an APD detecting an incident photon and being sensitive to a subsequent photon is known as the dead time or recovery time. Considering the detector in isolation, this is the time between an avalanche being initiated and being quenched and is therefore affected by the quenching electronics (see section 2.3). However, often counting or discriminating electronics have much greater deadtimes and therefore play more of a significant role [13], meaning the dead time of the entire detector chain needs to be considered. This is an important parameter for QKD as it determines the maximum count rates the detector can achieve and is thus directly related to the secure key rate.

Timing jitter

The statistical variation in the time between photon absorption and an electron being detected is known as the timing jitter, or timing resolution. This also includes any jitter from the corresponding electronics and so more accurately refers to the jitter of the

entire detector system, but in general the detector jitter dominates [99]. Higher electric fields, and thus higher excess voltages, have been shown to decrease the jitter with the added consequence of higher dark count rates and higher detection efficiencies. [107, 108]

The detector diameter also has a significant impact as this dictates the area over which the avalanche spreads such that the diode becomes conducting, meaning larger area devices have a larger jitter [108]. Detectors with a large jitter increase the possibility of intersymbol interference occurring and can result in an increased QBER and therefore a reduced secure key rate.

Photon number resolution

It is also useful to consider whether a detector is capable of distinguishing photon number. This can add an extra level of security against photon number splitting attacks [109], not to mention being essential for other quantum information applications, such as linear optics quantum computation [110]. Multi-pixel APDs for visible wavelengths have already been shown to demonstrate impressive photon number resolution [111, 112], however devices have yet to reach a similar level of maturity for detectors sensitive in the near-infrared [113]. Having said that, limited photon number resolution has been achieved with single pixel devices [114–116] and utilising such devices for detecting photon number is appealing due to the fact that there is no loss of detection efficiency as a result of geometric fill-factor [111].

The above characteristics can be grouped together to give an overall figure of merit which can be useful for assessing an APD, several of which are covered in [117] and [99]. It is however often not possible to make direct comparisons between detectors due to factors such as geometry, existence of pixels and values quoted at different parameters (e.g. detection efficiency measured at different temperatures or at different dark count rates). As such, there cannot be one, universal way of quantifying the merit of detectors and they should be chosen based on their desired application.

2.3 Operational regimes for APDs

Although APDs are widely used in classical optical communications [118], the conditions under which they are operated for such an application are vastly different to those used for QKD. The difference between the two is best explained by considering an I-V curve of an APD, as shown in Fig. 2.2.

For classical communication, the device is operated in linear mode. This regime occurs above the APD punch through voltage, where the gain is unity and impact

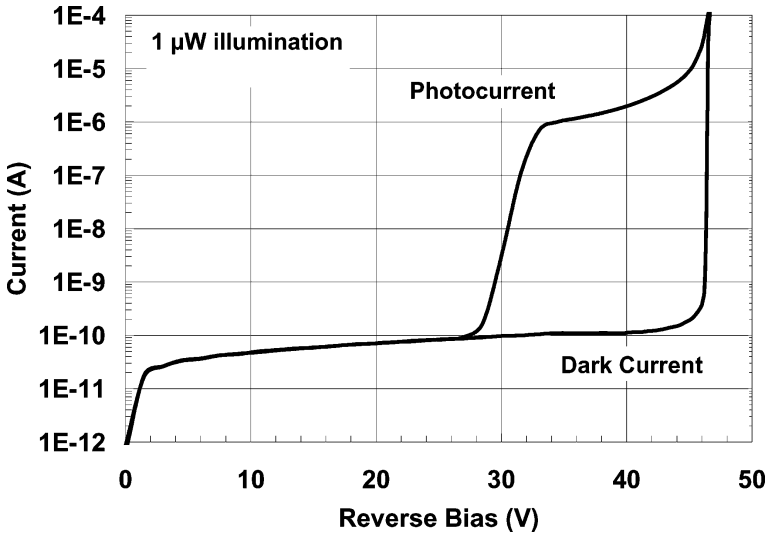


Fig. 2.2 **I-V** *curve of a device characterised under dark and illuminated conditions from [1]. The first shoulder under illumination indicates the punch through voltage, where the gain of the device is unity. Above this voltage, the APD is said to operate in linear mode. The breakdown voltage is given either by the second shoulder under dark conditions, or when the dark current reaches* $1\mu A$*. APDs for single-photon detection are usually biased above this value.*

ionisation begins to occur, and is shown by the initial shoulder under illumination in Fig. 2.2. When used in telecommunication applications, the gain is usually between 1 and 100 [118]. In the linear regime, the number of generated carriers is proportional to the number of absorbed photons, hence the relationship, and the mode, is linear [1].

When biasing the device further, the APD reaches its breakdown voltage, which is variously described as either the shoulder under dark conditions where the dark current suddenly increases [119] or when the dark current reaches 1-10 μA [1]. Above this particular voltage, a generated avalanche under impact ionisation now becomes self-sustaining. This results in an individual photon generating many more carriers, enough to produce a macroscopic current detectable by conventional electronics. This regime is known as Geiger mode, so named due to its similarity in behaviour to Geiger-Müller tubes [101].

Due to the self-sustaining nature of the avalanche, it is necessary to quench the avalanche to protect the device from damage but also to prime it for future detection [120]. A number of techniques have been developed and are outlined below.

2.3.1 Passive quenching

The earliest and simplest technique for quenching an avalanche is to do so passively, with a resistor placed in series in the APD biasing circuit. When a photon is detected

and the current in the device rises, the resistor automatically quenches the avalanche and primes the device for the next detection event. Due to its simplicity and the lack of necessity for any active circuitry, this procedure is employed for detectors operated in free-running mode where the bias voltage remains constant over time and the detector is sensitive to photons at any time interval. Despite its ease-of-use, the reset or quenching time of detectors operated this way can be problematic as it is related to the capacitance and bias resistance (or time constant) in the circuit [120]. This means that large key rates are not usually achievable due to low count rates on the order of kHz [121, 70].

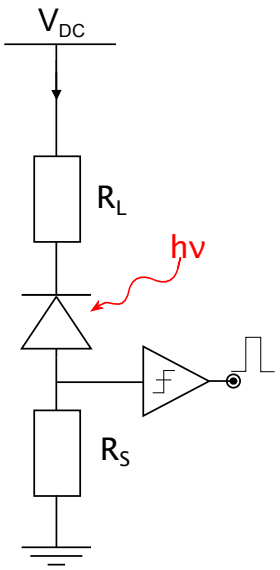


Fig. 2.3 **Passive quenching**. *The earliest and simplest technique for quenching an avalanche. A large bias or load resistor is used to reduce the voltage below the breakdown voltage, and thus quench the device. V_{DC}: DC voltage; R_L: Load resistor; R_S: Sensing resistor.*

2.3.2 Active quenching

In order to combat the slow recovery times exhibited by passively-quenched APDs, active quenching was developed [122]. This technique involves sensing the rise of the avalanche and 'reacting back on' the APD and quenching it [107]. The existence of this feedback loop, where a comparator senses the rise of the avalanche and switches the output voltage to a value above or below the breakdown voltage depending on the current sensed, is the significant step that separates active from passive quenching. The switching is usually implemented by means of a fast transistor, however circuits can easily have a significantly larger amount of complexity. Count rates can be larger

than passively-quenched APDs [123] but still fall short of the GHz level that can be achieved using gated quenching [124] described in section 2.3.3.

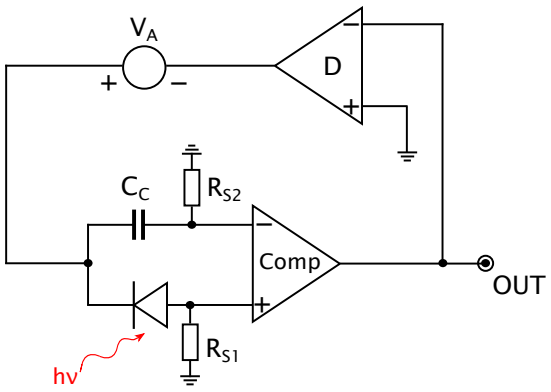


Fig. 2.4 **Active quenching**. *Circuit reproduced from [81]. V_A: Applied voltage; D: Fast switch; C_C; Capacitor; R: Resistor; Comp: Comparator.*

2.3.3 Gating

For QKD, APDs are usually operated in gated mode, as the arrival times of photons from Alice only occurs in discrete time windows. This involves periodically biasing the device above and below the breakdown, thus producing 'ON' times, where the APD is primed for detection, and 'OFF' times, where it is insensitive to single photons and the avalanche is quenched. It is common for this to be done with either square waves or pulses.

An example of an early implementation of this technique is the coincidence method [125, 126]. This way of performing gating involves essentially correlating detection events with the 'ON' time of the gating signal by means of a logic AND gate. However, to minimise the effect of registering electronic noise, the discrimination level is usually set quite high, meaning weak avalanches avoid detection. This becomes problematic when devices are biased at higher gating frequencies that would be desirable to achieve higher count rates for QKD as the capacitive response would be of a comparable magnitude to the avalanches, making discrimination difficult. In such cases, where 'ON' times are short, avalanches have less time to build up and so would be too weak to be detected. As discussed in section 2.2.1, a further incentive for having shorter gates is the existence of additional spurious counts that are correlated with legitimate detection events, known as afterpulsing. The exact nature and origin of these afterpulses is still an open question, but generally they are attributed to deep traps in the multiplication layer [104, 119, 127]. For this reason, limiting the avalanche charge by having shorter

gates is desirable but additional background cancellation techniques needed to be developed, as outlined in the following sections.

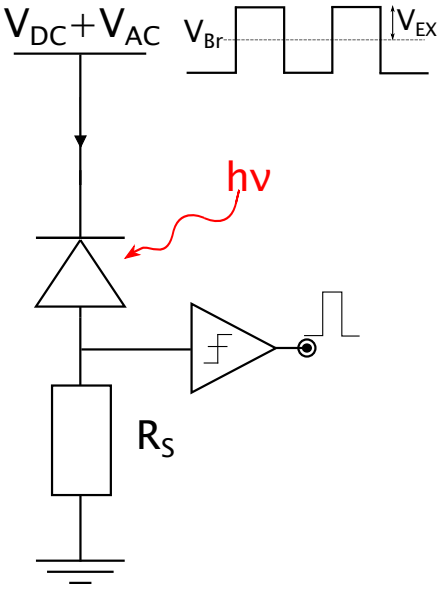


Fig. 2.5 **Gating** *scheme for a single-photon APD, where the detector is periodically biased above and below its breakdown voltage, the amount of which is known as the excess voltage. The AC signal is combined with a constant DC signal to drive the device.* V_{DC}*: DC voltage applied to the device;* V_{AC}*: AC signal;* R_S*: Sensing resistor;* V_{Br}*: Breakdown voltage;* V_{EX}*: Excess voltage.*

Sine-wave gating

One technique for achieving good APD performance at high gating frequencies is to use a sine wave instead of a square wave or pulse for gating the detector. This means that the capacitive response can simply be neglected using a cascade of band rejection filters centred at the gating frequency, thereby making it straightforward to discriminate avalanches from the background.

APDs operated in this way have shown promising results with gating frequencies exceeding 1 GHz [128, 129, 71], detection efficiencies as high as 30 % [71] and afterpulse probability less than 1% [130]. Although these achievements, in addition to significant developments such as miniaturisation of the APD module [71], are impressive, the performance of such detectors still falls short of those using the self-differencing technique.

Self-differencing

Developed in [131], self-differencing (SD) is a type of background cancellation technique usually employed with square-wave gated detectors. The output of a gated detector is first split in half. One of the two halves is then delayed by a gating period (i.e. 1 ns for a 1 GHz gated detector). The two arms are then recombined, which results in the cancellation of the majority of the capacitive response, leaving a positive and negative signal which can easily be discriminated from the residual background, as shown in Fig. 2.6.

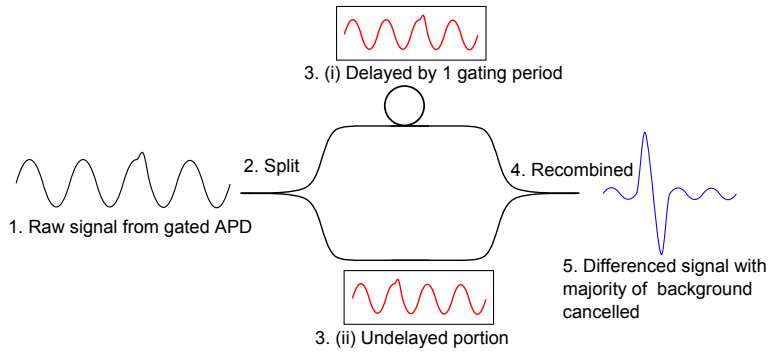


Fig. 2.6 **Self-differencing** *Outline of a self-differencing circuit. The output of a gated detector is split in half and one arm is delayed by a gating period (e.g. 1 ns for a 1 GHz gated APD) and the two arms are then recombined. This leaves a positive followed by a negative signal that are clearly distinguishable from any remaining noise.*

Thus far, InGaAs APDs operated this way have achieved the highest detection efficiency of 55% [68], record count rates of 1 GHz [132] and facilitated record secure key rates of up to 13.7 Mbits/s in QKD [13]. As such, they can be considered the state-of-the-art and are the focus for the work outlined in this thesis.

Significantly, due to the cancellation technique, APDs with SD circuits cannot detect consecutive avalanches, hence the theoretical maximum count rates of an SD APD is half its gating frequency. As outlined earlier, due to the unavailability of suitable single photon sources, under ordinary QKD operation Alice employs weak coherent pulses. These have an average flux of less than 1 to reduce Eve's ability to take advantage of the Poissonian nature of the pulses and perform the photon-number-splitting attack. As such, even when neglecting decoy pulses, the probability of consecutive pulses becomes very small, particularly at longer distances.

However, this particular characteristic of SD APDs can be exploited by Eve to perform a detector control attack. She can force Bob's APD to register avalanches in each gate, thus causing complete cancellation. She can then send her own strong pulses

and thus have control over when Bob's detectors click. This is a class of blinding attack, which it is helpful to briefly review before exploring this attack further.

2.4 Vulnerabilities of InGaAs APDs in QKD

2.4.1 Detector attacks

The single-photon detectors at Bob are the most vulnerable component within a QKD system due to their exposure through the quantum channel. This allows Eve the opportunity to manipulate the signal Bob measures in an effort to extract the secure key. Whilst a conventional intercept-and-resend attack won't work, a modified variant of this, known as the faked-state attack [133] has been demonstrated to be effective , insomuch as Eve can extract some or all of the key without alerting the users to her presence [134]. This involves forcing Bob's detectors to click only when he chooses a compatible basis with Eve. This relies on his detectors acting as threshold detectors, whereby they always click with an optical power above a certain value, and never when below it, which we denote as P_{th}. This is most clearly explained by considering passive-basis choice polarisation encoded BB84. Bob uses 4 detectors in 2 pairs, corresponding to the rectilinear and diagonal bases respectively. It is assumed these detectors are made to behave as threshold detectors, through blinding or any other mechanism. Say Eve has measured the qubit sent by Alice in the vertical polarisation using a copy of Bob's setup. She then encodes her faked pulse with her measured polarisation and configures it to have an optical power of twice the amount required to make Bob's detectors click, $2P_{th}$. This is split in half at the first beamsplitter, directing P_{th} down each arm. At the diagonal basis detectors, the power is split again at the polarising beamsplitter as it corresponds to an incompatible basis. Each detector sees a power of $\frac{P_{th}}{2}$ and therefore neither of them register a click. At the rectilinear basis detectors, all the power goes down one arm and only the corresponding detector clicks, thereby giving Eve and Bob perfectly correlated bits. This is outlined in Fig 2.7.

Whilst attacks have been investigated targeting a number of detection mechanisms, such as homodyne detectors for CV-QKD [135], superconducting nanowire single-photon detectors (SNSPDs) [136, 137], and even photomultiplier tubes [138], those involving avalanche photodiodes (APDs) are the most prominent due to their widespread use and promising characteristics for later commercial implementation. Although silicon APDs have attractive characteristics such as very high detection efficiencies (>70%) [139], their spectral sensitivity does not extend to the telecom C- and O-band regions [61], making them unsuitable for use in fibre-based systems.

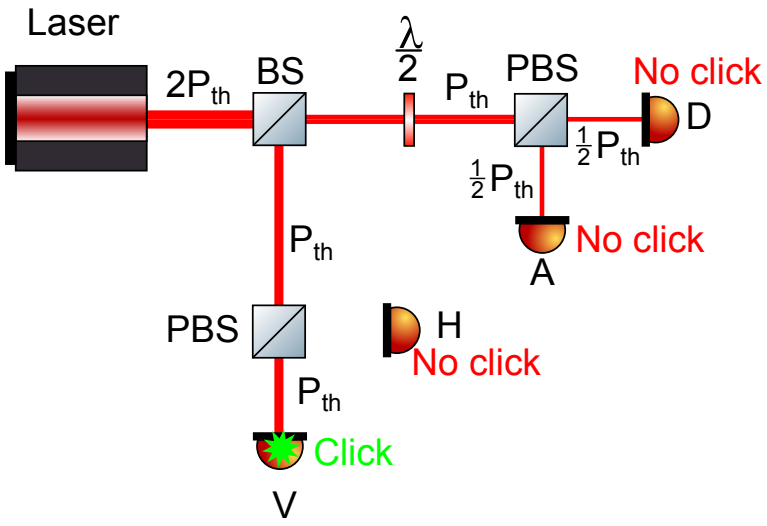


Fig. 2.7 **Faked-state attack** *Shown on a passive basis choice BB84 setup. Each pair of detectors corresponds to a particular measurement basis, in this the rectilinear and diagonal bases denoted by "H" ,"V" , "D" and "A". P_{th} corresponds to the the threshold power required to make Bob's detectors click. Eve sends a trigger pulse encoded with the "V" state with power $2P_{th}$ and thus guarantees detector "V" clicks.*

Since development of InGaAs/InP APDs has resulted in them being viable candidates for fibre-based QKD, so have the level and sophistication of attacks against them increased.

The most prominent implementation of the faked-state attack is performed by blinding the APD [134, 140–142], whereby Eve renders Bob's detectors insensitive to single photons but still responsive to strong, trigger pulses which she uses to control when they click. This attack provides a large focus of this thesis and will therefore be discussed further in detail later (see section 3.2).

Eve also has a selection of other detector attacks in her arsenal with which to target a QKD system. Due to unavoidable manufacturing and electronic deviations, Eve can exploit the temporal difference in efficiency that arises between multiple detectors in Bob's set-up [143]. This can be exploited actively, using the faked state attack [143], or more passively, whereby Eve simply controls the arrival time of Alice's photons, thereby making Bob more likely to register a particular bit depending on whether Eve delays Alice's photons or not [144]. This is shown in Fig. 2.8. She is introducing a deviation in the detectors from their theoretical behaviour, where it is assumed that the detection probability is independent of the bit or basis used.

An often overlooked potential loophole can present itself during the calibration routine before key distribution takes place [145, 146]. The goal is for the users to tune the arrival time of Alice's photons on Bob's detectors such that they register the

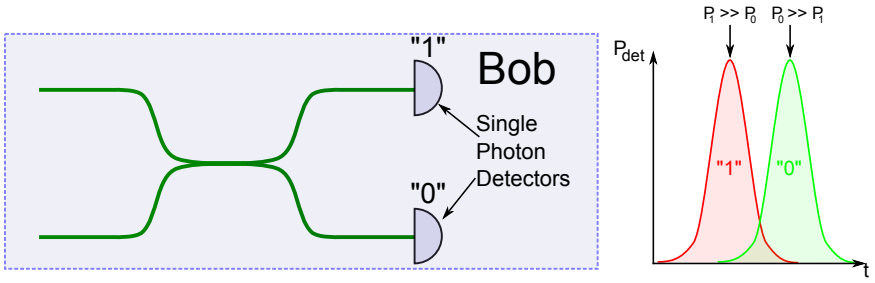


Fig. 2.8 **Detection efficiency mismatch** *Schematic of Bob's receiver set-up and the detection response of his detectors as a function of arrival time. If Eve can control the arrival time of qubits to Bob's setup (either the original ones sent by Alice or her own faked states) she can bias which detector clicks.*

maximum possible detection efficiency. This procedure can be exploited by Eve to introduce a temporal mismatch in the detectors' efficiency, thereby allowing her to perform the aforementioned time-shift attacks once key distribution is performed.

2.4.2 Other attacks

Whilst detector attacks are often the centre of focus for security concerns, other components in a QKD system are also vulnerable. Outside of the PNS and Trojan Horse source-based attacks discussed earlier, the technique used for switching between signal, decoy and vacuum states can also introduce side-channels. Typically, Lithium Niobate-based ($LiNbO_3$) Mach-Zehnder interferometers (MZIs) are used for producing the aforementioned states needed for performing the decoy-state technique used to protect the users from the PNS attack. However, patterning effects that arise due to intensity correlations between a particular pulse and its predecessor can leak information that Eve could use [147]. Further issues due to the ambient conditions surrounding the IM [148] can also arise. Moreover, performing decoy states by adjusting the pump current to the laser diode used as Alice's source does not produce pulses that completely overlap temporally [149], opening another backdoor for Eve. Using a Sagnac intensity modulator has been demonstrated as a solution to all of the above issues [150] but it is yet to be used in a full QKD system or subjected to intensive security testing.

It has also been shown that Bob's beamsplitters (BS) used for passive basis choice can be vulnerable [151]. Current technology results in a wavelength dependence of his BS, hence by tailoring the spectrum of her input light, Eve can control Bob's detectors in much the same way as a faked state attack and introduce a negligible increase in the QBER. This attack can easily be avoided with the use of active-basis choice QKD protocols such as [19].

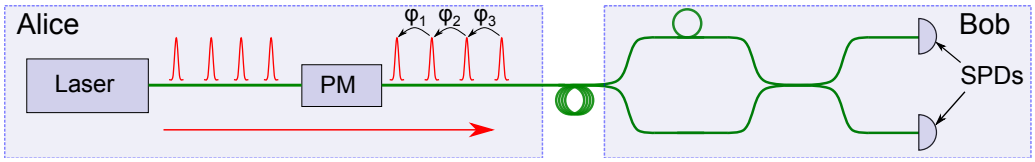


Fig. 2.9 **Differential Phase Shift** *Schematic of the DPS protocol, where qubits are encoded on the differential phase difference between subsequent pulses. PM: phase modulator; SPD: single photon detector*

2.5 Vulnerability of QKD protocols

The choice of QKD protocol can have a direct impact on Eve's ability to control Bob's detectors. Due to their simplicity and widespread use, BB84 and its variants are usually analysed when considering detector attacks, for example in the faked state analysis illustrated in Fig. 2.7. Although the vulnerability of distributed-phase reference protocols to faked state attacks has been examined in [152], it is useful to analyse each scenario in detail here.

2.5.1 Differential phase shift

We first begin with the differential phase shift (DPS) protocol first proposed in [153], refined in [20] and experimentally demonstrated in [154]. This encodes information in the differential phase between consecutive pulses sent by Alice. An attractive feature of the protocol is its simple implementation, as only a single basis is used, meaning each pulse is either encoded with a 0 or π phase shift. A 0 or 1 bit then corresponds to either no or π phase modulation respectively. Furthermore, it is inherently secure against the photon number splitting attack, meaning Alice does not need an intensity modulator with which to generate decoy states.

Alice therefore needs only a light source that emits photon pulses which maintain coherence with one another, a phase modulator for encoding her qubits and finally an attenuator to bring the pulses down to the single-photon level. Bob uses a passive asymmetric MZI (AMZI), with the delay corresponding to the time period of Alice's pulses and a single-photon detector at each output port. This is schematically shown in Fig. 2.9. He records which detector clicks and the corresponding time stamp for each click. Bob then tells Alice his timing information and in this way they can share a secret key.

Eve cannot perform a simple intercept-and-resend attack since she doesn't have access to Bob's measurement times, meaning she can't simply use copies of Bob and Alice's apparatuses. However, she can still perform her faked state attack assuming the

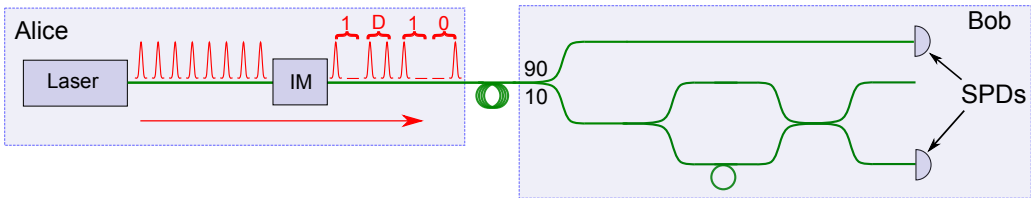


Fig. 2.10 **Coherent One Way** *Schematic of the COW protocol, showing time-encoded qubits with decoy states using pulse pairs. IM: intensity modulator; SPD: single photon detector*

detectors have a state that can be accessed where they click with a high probability with optical power P_{th} and low probability with $P_{th}/2$ (for example, if they are blinded).

Let's assume Eve wants to make detector 2 click. She sends a pulse with optical power P_{th} with no phase modulation, followed by a pulse with the same power with a π modulation. The first pulse is split at the first BS and $P_{th}/2$ travels down each arm. The pulse travelling down the short arm is then split again as no interference is occurring at the second BS so each detector sees an optical power of $P_{th}/4$ and neither one clicks. In the next case, a pulse of power $P_{th}/2$ with modulation 0, which has travelled through the long arm, interferes with a pulse of power $P_{th}/2$ and modulation π. As these two pulses have different modulations, they both go down the arm to detector 2 and it sees a pulse of power P_{th} and clicks, whereas detector sees no optical power and doesn't click. Therefore Eve's attack is successful and a countermeasure would be necessary.

2.5.2 Coherent one way

Another significant protocol worth discussing is the coherent one way protocol (COW). This is a time-bin encoding technique first developed by a group in Geneva in [155] and experimentally demonstrated in [17, 18]. Alice encodes her information in pulse pairs where a pulse-vacuum or vacuum-pulse correspond to a 0 or 1 respectively. She also uses a decoy state that consists of a pulse-pulse pair. Bob's receiving apparatus consists of two parts separated by a beamsplitter, where one part consists of a single-photon detector for measuring the arrival times and thus extracting the secure bits (top arm) and the other contains an AMZI with a detector placed at one output port (bottom arm) and is used for monitoring the coherence for the purpose of detecting an eavesdropper. Typically this is an unbalanced ratio where only 10% of the bits are used for measuring the coherence [18] and is outlined in Fig. 2.10. After Bob measures Alice's photons, he informs her of his timing information and Alice tells Bob when she sent decoy states allowing them to share a secure key.

In order for Eve to perform a successful attack, she needs to have control of both detectors. Assuming she carries out a blinding attack, she would need to send a blinding power of $10P_{blind}$ to control each detector, where P_{blind} is the minimum power required to blind an individual detector. This already presents an experimental challenge as it requires her to have detailed knowledge of the blinding regimes such that she ensures both P_{blind} and $9P_{blind}$ fall in this region.

Once under control, making the top detector click at will is possible using a power of P_{th} that ensures his detectors always click. Furthermore, obtaining a correlated set of bits with Bob is more straightforward than in BB84 as Eve does not need to worry about the case where Bob's detectors see $P_{th}/2$ which usually corresponds to mismatched bases. The difficulty for her would arise in maintaining the coherence and count rate measured by the bottom detector, particularly since she has no prior knowledge of whether Alice has sent a decoy or signal state and would thus introduce a mismatch after Alice and Bob have carried out their public announcements after key exchange. Whilst this suggests that a countermeasure to blinding would not be required, the lack of a security proof covering coherent attacks for the COW protocol does not necessarily make it more appealing than BB84 or T12.

2.6 Summary

In this chapter, a background to avalanche photodiodes in QKD was presented. The various quenching techniques used for APDs have been explained, illustrating a timeline of development and demonstrating the drawbacks with each method. It was shown how Eve could exploit the operating principles in order to control the detectors, as well as how the choice of protocol affects her ability to do so. The knowledge of quenching techniques of APDs and their structure are important for understanding the content of the following chapters, the first of which focuses on the best practice for operating self-differencing APDs to mitigate the blinding attack in QKD.

Chapter 3

Minimising vulnerabilities of self-differencing APDs through best practice

3.1 Introduction

Single-photon detectors are one of the most critical components for QKD. Indeed, the overall performance of a QKD system is directly related to particular characteristics of these devices. For example, the detector dark count rate has a significant impact on the maximum achievable distance over which QKD can be performed. However, the particular figures depend greatly on the choice of various settings of the device. Furthermore, choosing avalanche photodiode (APD) parameters not only affects the performance but also the security. This chapter focuses on the best practice for configuring a self-differencing APD in order to maintain its practical security.

3.2 Blinding

As discussed, Eve cannot perform an intercept-resend attack due to her ignorance of the states Alice sends. A modified version, known as the faked state attack, can succeed if she ensures Bob's detectors only click when his basis choice is aligned with Eve's [133]. Practically, this means Eve must be able to have some control over his devices such that she can make them register a count at will. The most thoroughly explored means of performing this is by means of blinding. By rendering Bob's detectors insensitive to single-photons but still able to detect strong optical pulses, Eve

can have complete control over his detectors without causing a significant increase in the QBER. In this way she can learn all of the key and remain undetected [134].

The first demonstration of blinding was carried out on a selection of passively-quenched APDs [140]. Such an attack works by bringing the device below its breakdown voltage, such that it is no longer sensitive to single photons. By shining strong light onto the detector, a large photocurrent is generated. Due to the existence of the large bias resistor which performs quenching, a large voltage drop is introduced and the device enters linear mode. By sustaining this level of current with a continuous wave (CW) laser, the bias remains below breakdown and the device is continuously quenched. This is a fundamental concept and is central to a large portion of blinding attacks.

Other techniques for forcing the APD into linear mode have also been explored. One of these is thermal blinding [156], which arises due to the fact that bright light required for blinding would also cause a heating of the device. As a result of the breakdown voltage's temperature dependence [68] (0.1 V/K is typical, see Fig. 5.4), when made hot enough, the device would cease to be operating in Geiger mode once more, and again be no longer sensitive to single photons. This occurs due to the increased lattice vibrations, also known as phonon scattering [157], as a result of a higher temperature which causes an increase in probability that a hole (or electron) collides with the lattice and loses its energy. As a result, there is a drop in probability that the hole gains enough energy to trigger ionisation of a new electron-hole pair. Therefore, in order to ensure the hole has enough energy, the electric field must be larger than the initial value of the breakdown voltage.

A more extreme case of using bright light to attack detectors is to use a laser so powerful that it actually damages the APD and thus introduces vulnerabilities in the system [158]. The authors of [158] were able to cause the same kind of blinding as in [141], whereby the detector is insensitive to single photons but still able to detect moderately bright light by damaging the detector. The advantage of this is that once blinding has been achieved the APD no longer needs to be controlled through illumination by Eve. Naturally this attack can easily be detected if Bob re-characterises his devices but it still opens the door for Eve, who could use such a technique to possibly target any 'watchdog' detectors used as security countermeasures [159].

Although a significant body of work demonstrating blinding has been published [134, 141, 142], it is important to make the distinction between a genuine loophole and simply inappropriate operation. This point was first made in [160] and later expanded upon in [161]. With regards to gated APDs, the detectors of choice for the system under scrutiny (IDQuantique's Clavis2), two main criteria are clear:

1. Do not use a high-impedance bias-resistor
2. Set the discrimination appropriately

Additionally, since Eve's blinding power is typically many orders of magnitude greater than that used by Alice for sending her single photons, monitoring the APDs' photocurrent is also an effective measure. The most prominent demonstrations of blinding [134, 141] violate one or both of the above criteria. Furthermore, at least one study published after [161] shows blinding on an APD operated with an inappropriately high discrimination level [142, 162], thereby highlighting the need for further work on this subject.

3.3 SD blinding

As discussed earlier, due to the cancellation of the SD, it is impossible to discriminate two consecutive, identical avalanches. In theory, this effect can allow Eve to completely blind the detector with a moderate optical power. By illuminating the APD with CW light of sufficient intensity, it is possible to deterministically produce an avalanche within each gate, thereby forcing a complete cancellation of avalanche signals and bringing the detection count rate to zero [162, 163]. Assuming identical avalanche amplitudes, the detection probability (P_{det}) and count rate (CR) can be simulated using

$$P_{det} = (1 - e^{-\mu\eta}) \cdot e^{-\mu\eta} \tag{3.1}$$

$$CR = fP_{det} \tag{3.2}$$

where μ is the photon flux per pulse and η is the single photon detection efficiency. The first term of Eq. 3.1 is the probability that an avalanche occurs in a gate. The following term is then the probability of no avalanche occurring in the following gate. It can be seen that as $\mu\eta$ becomes very large, the second term, and therefore the whole expression, tends to zero.

We can estimate the optical power required to blind a conventional gated detector with the mechanism described in section 3.2. The actual excess voltage whilst the APD is under illumination can be described with the following

$$V'_{ex} = V_{ex} - I \cdot R_{bias} \tag{3.3}$$

where I is the generated photocurrent. This shows that if both I and R_{bias} are reasonably large, it is possible to make V'_{ex} zero or negative. This highlights the importance of

making R_{bias} as small as possible. However removing the bias resistor does not cause this to be zero as an intrinsic resistance exists in the circuit which we measure to be approximately 1 $k\Omega$ (see section 3.5).

Assuming an excess voltage of 4.4 V, an incident optical power of larger than 4.4 mW is required to bring the APD out of Geiger mode. By examining Eq. 3.1, we can see that an incident optical power of just under 60 nW is sufficient to blind a 1 GHz gated SD detector (assuming a pulsed laser of the same repetition frequency and a detection efficiency of 10 %), nearly 5 orders of magnitude smaller. Since the required optical power for blinding an SD detector is much smaller, it makes detection of an eavesdropper through monitoring of the photocurrent [161] less straightforward.

The body of work surrounding attacks on QKD systems is vast and beyond the scope of this thesis. As such, I refer the reader to a recent review article for more information [164].

3.4 Experimental setup

To test the effectiveness of SD blinding, a fiber-coupled InGaAs/InP APD was chosen. It was thermo-electrically cooled to -30 °C as this is an often used temperature for QKD experiments where the dark counts are reasonably low. Generic electronics in the form of a source measure unit (SMU) and pulse generator coupled to a bias tee are used to provide the SD-APD with the DC and AC biases, respectively. A variable quenching or biasing resistor is applied in the biasing circuit for later convenience and its initial value is set to zero. A continuous wave distributed feedback (DFB) C-band laser was used to illuminate the APD and the output was amplified by two 20 dB amplifiers. A schematic of the set-up used is shown in Fig. 3.1 (a).

Typically, APD avalanches are discriminated with either specially designed photon counters and/or front-end electronics and then counted with field-programmable gate array (FPGA) electronics or the same photon counter [13, 39]. These are well-suited to QKD applications when count rates are relatively low. However, when high optical powers are applied to the device for characterising blinding, the count rates become far greater and can exceed the maximum ratings that such counters can cope with. Indeed, in this study, several solutions for measuring count rates were tested, but they either resulted in saturation of the photon counter or prohibitively long measurement times. As a result, a 16 GHz oscilloscope was used to extract individual waveforms and these were then discriminated by a purpose-built LabView programme. Such a technique proved able to cope with the large count rates (up to 1 GCounts/s) at reasonable speeds

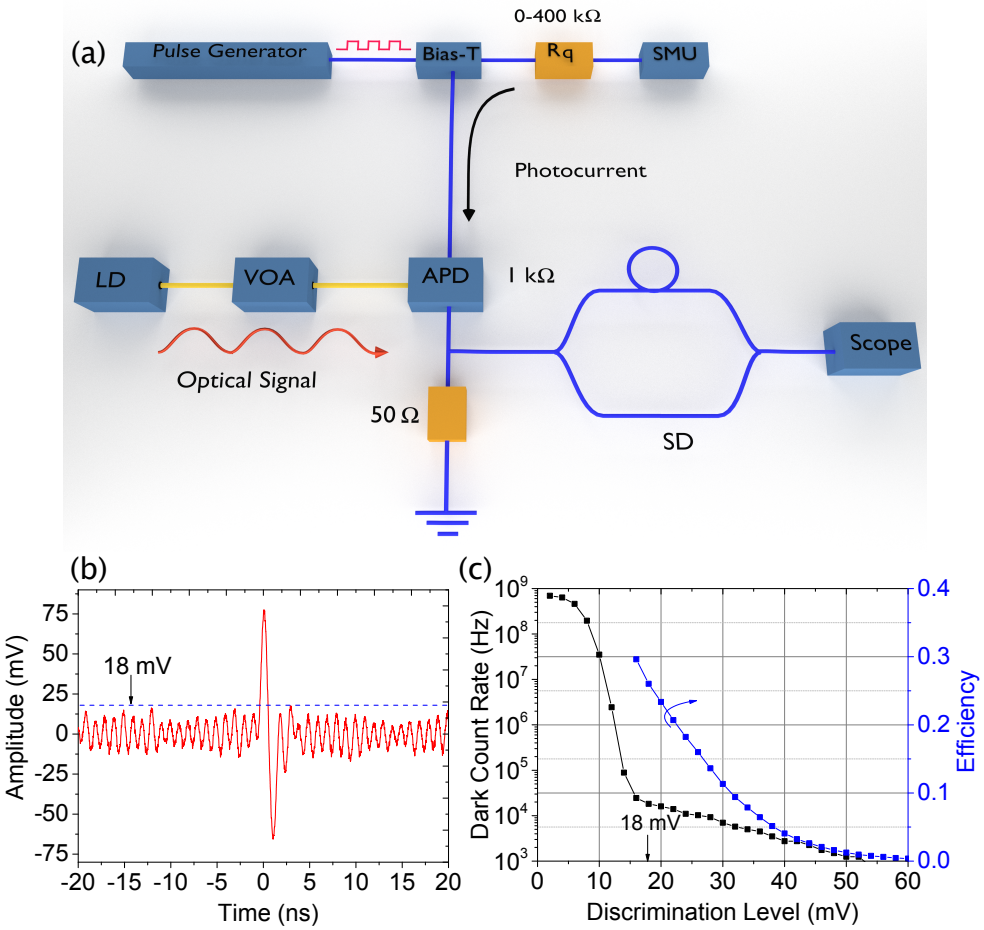


Fig. 3.1 **Setting up the APD** *(a) Setup for characterising the self-differencing detector under bright illumination. LD: laser diode; VOA: variable optical attenuator; SD: self-differencer; Rq: quenching resistor; SMU: source measure unit. (b) An SD output waveform showing a single avalanche rising above the capacitive response residual. (c) Detection efficiency and dark count rate as a function of the discrimination level. 18 mV is marked as our chosen appropriate discrimination level.*

with the added bonus of providing a more direct control over the discrimination level used for the counting of avalanches.

Recapping from section 2.3.3, under fast gating, an APD produces a strong capacitive response which can be much stronger than the avalanche signals arising from photon detections. To suppress such a response and enable photon detection, the SD circuit splits the output of the APD in half, shifting one of those halves by a gating period and then recombining the two halves in order to cancel the strong capacitive response of the detector [131]. Fig. 3.1 (b) shows a typical waveform of an SD output, with an avalanche signal rising above the residual, uncancelled background of the detector capacitive response.

When first setting up the detector it is important to carry out a series of steps in order to systematically arrive at the most appropriate way of operating it. This prescription is given as follows:

- Determine the APD's breakdown voltage. This is taken as the point at which the generated current exceeds 10 μA [1] when the APD is biased with the DC signal only and without optical illumination. This was carried out using a source measure unit (SMU) by applying a current to measure the voltage. The breakdown voltage was found to be 51.8 V.

- Set the initial DC and AC biases. The initial DC bias is set at 51.6 V, just below the breakdown voltage, using the SMU in voltage mode. An AC signal applied using an amplified signal from a pulse generator is set at a sufficient level to enable single photon avalanches, i.e., approximately 5-10 V.

- Set a coarse discrimination level. This is set by lowering the DC bias such that the APD never experiences any excess bias and therefore does not produce any single-photon or dark counts. We use a value 10 V below our initial DC, i.e. 41.6 V. Under this condition, the SD output contains only the background signal. The coarse discrimination level is set as the lowest level with which the counting electronics produces a count rate of zero such that all of the background is neglected. This coarse discrimination level can then be used when varying the DC and AC signals to find the optimum detector characteristics as in the next step.

- Optimise the biasing conditions. This involves adjusting the DC and AC levels around $V_{DC}^{(1)}$ and $V_{AC}^{(1)}$ to optimise the detector performance, such as detection efficiency, dark count rate and afterpulse probability. The detailed procedure for this step can be found in a previous publication [68]. We refer to the optimised

bias values as $V_{DC}^{(2)}$ and $V_{AC}^{(2)}$. For this study, we chose values of 51.6 V and 4.6 V respectively. These bias condition result in an excess voltage of $V_{ex}^{0} = 2.1$ V over its breakdown voltage.

- Set the final discrimination level under the optimal biases of $V_{DC}^{(2)}$ and $V_{AC}^{(2)}$. This step is necessary because the capacitance of an APD is bias dependent and so is the uncancelled capacitive signal background. Under dark conditions, the detector count rate is measured as a function of the discrimination level. The point where the count rate changes dramatically signals the detection of the noise floor. Therefore, one should choose a discrimination level just above this to ensure an optimal detection efficiency while rejecting all uncancelled capacitive background contributing to the dark counts.

Figure 3.1 (c) shows the detector efficiency and dark count rate as a function of the discrimination level after the values of $V_{DC}^{(2)}$ and $V_{AC}^{(2)}$ have been chosen. The dark count rate shows a kink at the discrimination level of 16 mV, indicating the threshold above which the dark avalanches have replaced the capacitive residuals to be the dominant contribution to the measured dark count rate. While we could use this level, we set the discrimination level about 10% higher at 18 mV in order to have a tolerance margin.

The detector is measured to have a single photon detection efficiency of 26% for pulsed light and a dark count rate of $\sim$23 kHz for this discrimination level using a pulsed laser with repetition frequency of 15.625 MHz (1/64 GHz). Setting a higher discrimination leads to a lower detection efficiency and dark count rate. More detrimentally, this can also favour blinding, as we will show later, and therefore goes against the best practice of using SD-APDs.

For the purpose of this study, we use a relatively rough estimate for the detection efficiency using the following equation:

$$\eta = \frac{CR_{ill} - CR_{dark}}{F_{laser}\mu} \tag{3.4}$$

where CR_{ill} is the total illuminated count rate, CR_{dark} is the total non-illuminated count rate, F_{laser} is the laser repetition frequency and μ is the flux in photons per pulse. This uses a general measurement of the overall count rate, therefore it overestimates the detection efficiency as it includes afterpulses as legitimate counts. A more accurate technique is given in [95] however as characterisation is not the main focus of this study, the method using Eq. 3.4 is sufficient for our purposes.

3.5 SD APD under strong illumination

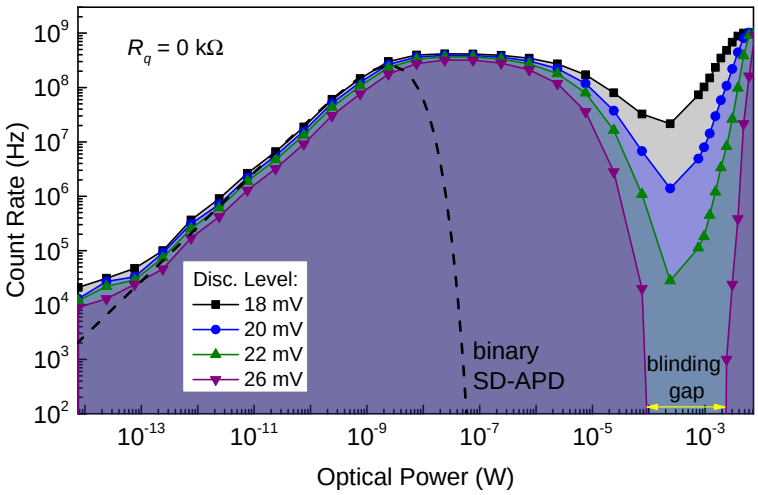


Fig. 3.2 **Effect of discrimination level on APD count rates** *Detector count rates as a function of incident optical power from a continuous-wave C-band laser diode with different discrimination levels. The variable quenching resistor is set to 0 Ω. The dashed line represents Eq. 3.2 with a constant* $\eta = 0.028$ *for continuous-wave illumination.*

To examine the blinding behaviour of the APD, we subject our detector to continuous-wave illumination from the laser diode. Fig. 3.2 shows the detector count rate as a function of the incident optical power for various discrimination levels. We first look at the result obtained with the appropriate discrimination level of 18 mV. In the weak illumination regime ($\leq$10 nW), the detector behaves like a typical single photon detector. Its count rate is initially dominated by dark count noise, then increases linearly due to detection of incoming photons before saturation at about 4 nW. Beyond saturation, the detector exhibits a count rate plateau between 10 nW to 2 μW while Eq. 3.2 predicts an immediate, sharp drop in the count rate. When the optical power is greater than 2 μW, the count rate starts to fall noticeably because of the SD cancellation between neighbouring gates. However, the fall only creates a shallow dip with a local minimum of 21.4 MHz at $\sim$ 0.23 mW. We do not observe detector blinding, *i.e.*, the count rate falling to zero for the incident power up to 7 mW.

By increasing the discrimination level, both the detection efficiency and saturation count rate become lower, as a higher discrimination level rejects a larger fraction of self-differenced signals. More strikingly, the count rate dip becomes deeper. At 26 mV, the detector registers a zero count rate with an incident power between 0.1 and 2.5 mW. The existence of this blinding gap makes Eve's blinding attack feasible, and this leads to an unsurprising conclusion that an inappropriately-set SD detector is vulnerable,

just like its low speed counterparts [161]. We note that the minimum blinding power is still more than three orders of magnitude larger than that predicted by Eq.3.2.

To understand the origin of the discrepancy, we perform another experiment by varying the resistance value of the quenching resistor in the DC path of the detector biasing circuit. While use of a quenching resistor is common for free-running APD detectors [165], it is unnecessary for gated APDs because an avalanche is automatically quenched after a detection gate.

For the purpose of obtaining an accurate value for the bias resistance, R_{bias}, of the APD in Eq. 3.3, the series resistance of the APD and electronics was measured. This was done by applying a small forward bias using the SMU with the AC from the pulse generator switched off and the bias resistance set to 0 and measuring the generated current. By calculating the gradient once the current starts to increase, the inverse of this results in the intrinsic resistance of the APD and the rest of the circuit, shown in Fig. 3.3. This was measured to be approximately 1.0 kΩ.

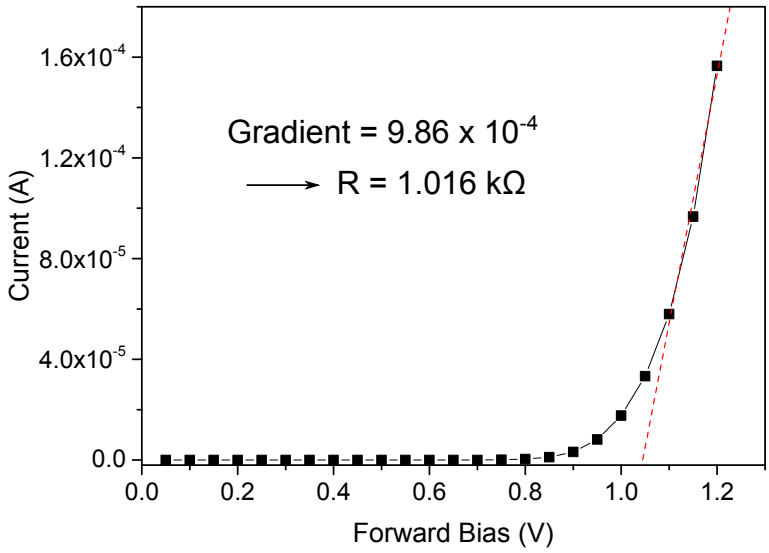


Fig. 3.3 **APD intrinsic resistance** *APD current measured under forward biasing conditions. By determining the gradient of the final three points, the intrinsic series resistance can be extracted and was found to be approximately 1 kΩ.*

Figure 3.4 (a) shows the count rate dependencies for different resistance values together with that obtained without a quenching resistor. Here, we choose to use the ill-set discrimination level of 26 mV to enhance the blinding effect. A blinding gap exists for all resistance values, but the gap shifts to lower power regions as the resistance value increases. With 400 kΩ, the blinding power is just 100 nW, which is three orders of magnitude lower than the 0 kΩ case.

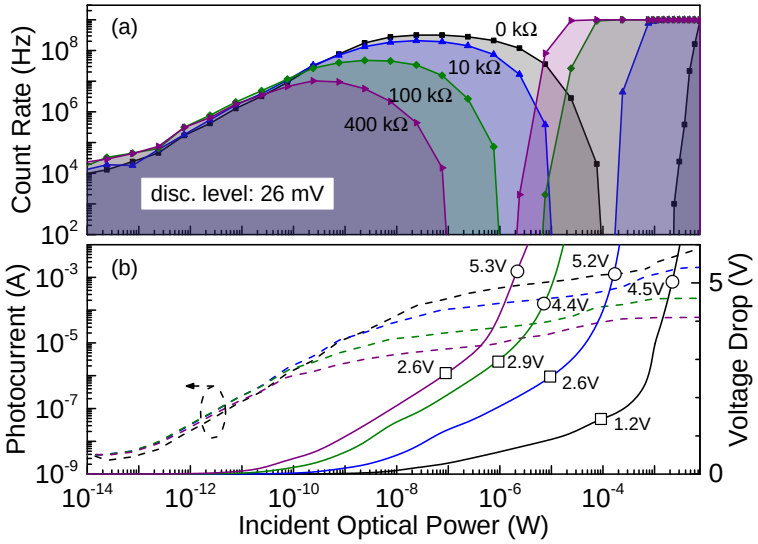


Fig. 3.4 **The impact of the quenching resistor** *Detector behaviour with different quenching resistor values. (a) Detector count rate as a function of the incident optical power at an ill-set discrimination level of 26 mV; (b) Measured photocurrent and calculated voltage drop in the detector bias. The same colour codes are used in (a) and (b) to represent different quenching resistor values.*

Figure 3.4 (b) shows the measured detector photocurrent using the SMU (dashed lines) as a function of the incident optical power. Flowing through the resistive components, including both the quenching resistor and the APD itself, the photocurrent creates a voltage drop and therefore lowers the detector reverse bias, see Fig. 3.4 (b) (solid lines). This has two direct effects. First, it reduces the avalanche probability (η). The higher the incident power, the lower the excess bias and avalanche probability. This explains why the detector requires a much higher optical power to become blinded than that expected from Eq.(3.2) and the formation of the count rate plateau. Second, it lowers the avalanche signal amplitude and consequently the differential signal between adjacent detector gates. A larger quenching resistor makes the detector excess bias drop faster, as shown in Eq. 3.3. The larger the value of the circuit resistance, which incorporates the bias and APD internal resistances, the smaller the required photocurrent to reduce the excess bias, V_{ex}, to zero, which results in an earlier blinding. The voltage drop corresponding to blinding is marked in Fig. 3.4 (b) with empty squares.

A third effect caused by the photocurrent can explain the count rate recovery shown in Fig. 3.4 (a). We mark in the figure the voltage values corresponding to the recovery point after each blinding gap with an empty circle. The voltage drop values are all around 5 V. This observation provides a key to understanding the count rate recoveries, as we explain here. A SD circuit suppresses the detector capacitive response but

will always leave a residual background due to its finite performance. The amplitude of such background is proportional to the APD capacitance, see Fig. 3.1 (b), which depends on the thickness of its depletion layer that is reverse-bias dependent [166]. A voltage drop leads to an increase in the capacitance and hence the amplitude of the residual background, which will eventually overcome the discrimination level and revive the counting rate. This explanation agrees with the count rate reaching 1 GHz for all quenching resistor values, see Fig. 3.4 (a).

To provide further support to this argument, we measure the APD capacitive amplitude under dark conditions before the SD circuit as we reduce the DC bias applied to the device. This was performed by varying the DC on the SMU and using an in-built function of the oscilloscope to measure the amplitude.

As shown in Fig. 3.5, we find that at the point of recovery, the response has increased in amplitude by 25% of its original value where there is a bias reduction of 4.5 V. This quantity of bias reduction can be realised using 2.3 mW of optical illumination for the case of the biasing resistor being set at zero. Due to the imperfect cancellation of the SD, the increased capacitance of the APD translates to a larger background after the SD circuit. This measurement result also justifies our choice of the appropriate discrimination level being only 10% above the capacitive background (see our previous discussion), as this can easily be overcome by such a dramatic increase in the residual capacitive signal. We note that the measured increase of the capacitive signal is applicable to all fast-gated APDs [130, 131, 167–171].

With both sides of each blinding gap accounted for, it is natural to understand the gradual disappearance of the blinding gap when lowering the discrimination level (Fig. 3.2). In a “blinding" gap, the SD output signal is made up of two components with opposing trends. The differential output of the SD circuit becomes smaller as the incident power increases, because each detector gate is more likely to produce an avalanche with a saturated amplitude or the amplitude itself is reduced by the lowered excess bias. Concurrently, the residual capacitive background gains strength due to the reduction of the APD reverse bias. The latter can overcome an appropriately set discrimination level before the photon-induced signal falls completely under that discrimination level.

The above explanation is distinctively different from gain modulation that has prevented conventional gated APDs from blinding [161]. Although still present, the modulation of the photocurrent by detector gating is periodical and considerably weaker than the capacitive response and therefore its contribution to the self-differencer output is negligible. Laser intensity fluctuations can also produce self-differencing signals that can overcome a detector discrimination level at high illumination power,

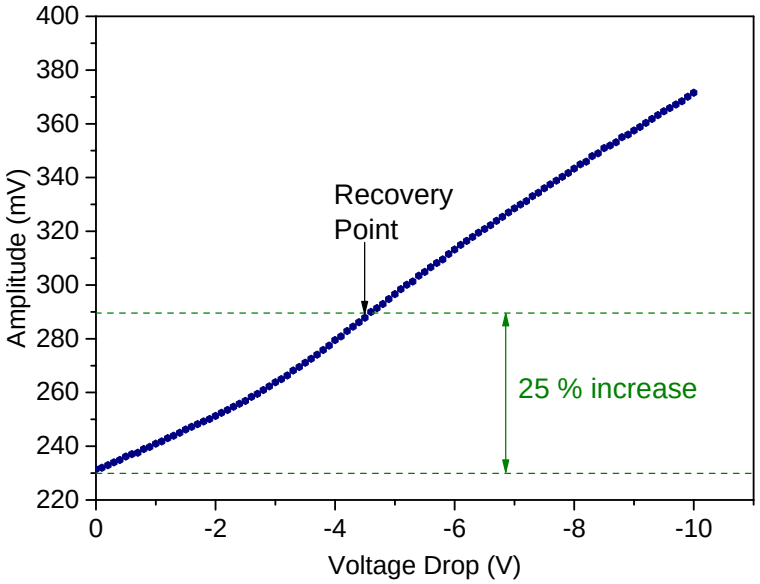


Fig. 3.5 **APD capacitive response** *measured before the self-differencing circuit as a function of the DC bias reduction below its normal value. We mark the point corresponding to the count rate recovery as shown in Fig. 3.4.*

in particular when pulsed optical excitation is used [162]. However, this mechanism does not play the dominant role in our case using continuous-wave illumination. First, it is incompatible with our observation in Fig. 3.4 that the recovery power can vary over three orders of magnitude for the same detector and blinding laser, with the lowest recovery power being merely 2 μW. Second, the intensity fluctuation should produce a maximum count rate that is half of the gating frequency, while we observed a maximum count rate of 1 GHz.

3.6 Best-practice criteria

We propose below a list of best-practice criteria to be followed in either designing or operating self-differencing detectors to mitigate blinding attacks.

- Monitor the photocurrent. The blinding current is still on the order of 1 mA, which can easily be sensed using a resistor of 1 kΩ.
- Avoid use of a quenching or biasing resistor of high resistance value, because it can provide overly strong feedback to the excess bias and therefore severely limit the maximum count rate. We recommend a value less than 50 kΩ when a biasing resistor is desired to limit the current for protecting the APD detector.

This resistance value will still allow a maximum count rate of over 30 MCounts/s and have a negligible effect on the QKD key rate.

- Set an appropriate discrimination level. This not only gives an optimal detection efficiency but also enables protection by sensing the excess voltage reduction through the residual capacitive background.

- Use different resistance values in a QKD system that contains more than one detector. A careful choice of resistance values can prevent an overlap of the detectors' blinding gaps, see Fig. 3.4, when their discrimination levels are inadvertently ill-set.

- Verify whether the capacitive response residual can overcome the detector discrimination level when the APD's reverse bias is lowered below its breakdown. If not, detune the self-differencing circuit slightly and/or re-set the detector discrimination level.

Compliance with the above criteria does not introduce a significant increase in system complexity nor a reduction in the secure key rate. This is an advantage as compared with the countermeasure of monitoring the detector efficiency [172], which offers a higher level of assurance but at the expense of the system simplicity and key rate. We note that the applicability of the proposed criteria is not limited to SD detectors, but extendable to other types of high-speed gated APD detectors, as discussed earlier. They can all improve their resilience from the negative feedback of the photocurrent, despite their use of different signal cancellation techniques.

3.7 Conclusion

In summary, we have experimentally studied the behaviour of an InGaAs self-differencing detector under bright illumination from a continuous-wave laser. We have shown that the intrinsic, negative feedback of the photocurrent has prevented not only an early blinding but also a complete blinding at very high attacking powers by strengthening the residual capacitive background. We have shown the importance of setting an appropriate discrimination level as this has a direct impact on the detector's behaviour under Eve's blinding attack. Our findings allow us to outline a set of best-practice criteria to ensure the most secure conditions to operate these detectors in QKD systems. Whilst these steps can ensure the practical security of the device, this is not a complete countermeasure. Furthermore, this theme has been briefly explored for gated APDs,

yet these detectors are still often inappropriately operated, hence it would be desirable to ensure security of SD APDs even when they are subjected to similar misuse.

Chapter 4

Using intensity modulation to prevent blinding

4.1 Introduction

In the previous chapter, mitigating blinding of an APD was approached by establishing the best practice for operating these devices. Whilst it was shown as effective for the device studied, this can only establish practical security, largely due to the deviation between APDs and attacking lasers. In order to come closer to obtaining an information-theoretic secure measure, more needs to be done. This chapter will concentrate on how an intensity modulator can used as an effective measure for eliminating blinding.

4.2 Previous countermeasures to detector blinding

A brief survey of blinding attacks targeting APDs has been presented in Section 3.2. Whilst the literature surrounding the finding of security loopholes in QKD systems is extensive, considerably less work is dedicated to presenting convincing countermeasures to these backdoors. This is perhaps a result of the difficulty in definitely *proving* a countermeasure is effective; indeed countermeasures can easily be refuted either because all attacks (known or unknown) are not considered or that an all-powerful Eve could subvert the countermeasure using, say, a quantum memory, which is beyond currently technology.

Countermeasures can be broadly divided into two categories, active and passive. In a passive approach, the legitimate QKD users (Alice and Bob) monitor in real time the device parameters that change under Eve's attack [172, 173]. In an active

approach, they add extra guarding components to thaw Eve's attempt [34, 174]. Using the Trojan-horse attack [33, 175] as an example, Alice and Bob can employ either a watchdog detector to actively detect Eve's presence [176] or a combination of an optical filter, attenuator and isolator to passively prevent Eve's light from reaching the encoding devices [34].

From the point of view of APD blinding, the most intuitive measure to combat blinding is an passive one and is to monitor the photocurrent generated by the APD [161]. As the optical powers needed for blinding gated APDs can be many orders of magnitude greater than the power used by Alice, the APD would generate a significantly larger current. However, as pointed out in [177], defining a magnitude of photocurrent which is a signature of Eve is problematic and ideally it should be incorporated into a security proof to guarantee the security. Indeed, this is a thorny issue and discussions surrounding blinding, distinguishing between incorrect operation and genuine loopholes, and countermeasures have been somewhat contentious [141, 142, 160, 161, 177–183].

Active countermeasures have also been explored, often involving manipulation of the APD gates. By randomly removing APD gates and essentially bringing the detection efficiency in those gates to zero, Eve would be caught as she would place clicks where there would be none in her absence [180].

A further option proposed has been from the point of view of modifying the design of the electronics [174]. This involved splitting the signal before the self-differencer splitter, such that a separate path could essentially be used for monitoring for blinding. The large optical powers required for blinding would mean that a comparator in this additional path could detect clicks without the need for a cancellation scheme. However, the attenuation in signal as a result of the second splitter has not been characterised and could degrade the signal-to-noise ratio, potentially reducing the secure key rate.

4.3 Modulating Eve's blinding laser

Here, we propose taking preemptive action against blinding by placing an intensity modulator (IM) in front of the receiver's measurement apparatus. The use of low extinction ratio modulation will not severely attenuate the incoming quantum signal, but the IM will create sufficient modulation in the detector's photocurrent, which is detectable by SD circuitry and discrimination electronics. We experimentally demonstrate this method on an SD InGaAs APD.

This idea is similar in spirit to the random variation of an APD's detection efficiency, suggested and partially implemented in [180], which was shown to be ineffective against a refined Eve's attack [142]. However, our proposal contains some notable differences. An APD endowed with an SD circuit sets a more challenging target to the eavesdropper. In fact, Eve has to send sequential light pulses with identical intensity to cause blinding. Any small deviation from this condition is likely to cause a detection event with an associated 50% quantum bit error rate (QBER). At the same time, a long sequence of bright optical pulses generates a high photocurrent which is easily detectable [160]. When an IM with random modulation is added on top of this already compelling situation, the constraints for Eve become extremely stringent. In particular, we found no room for blinding in our experiment.

4.4 Blinding attacks and countermeasures

As outlined in Chapter 2, single photon sensitivity of an APD relies on having an electrical excess bias above its breakdown voltage to enable avalanche multiplication of a single photo-carrier. In the blinding attacks, Eve erodes this excess by inducing an electrical current flowing through the biasing circuit [161] or heating up the device to raise its breakdown voltage [156]. These attacks are realised through injecting a strong laser signal into Bob's module through the quantum channel and making both of his detectors blind, i.e., insensitive to single photons. At this point, Eve performs a modified intercept-resend attack to take control of Bob's detectors. She measures the state prepared by Alice and re-sends a suitably prepared faked state encoded in a strong optical pulse. This will then trigger a detector count only when Bob chooses a measurement basis that is identical to Eve's. In this attack, Eve can gain full information about the final key [133].

Consider an APD detector operated in Geiger mode with an excess voltage of V_{ex}^{0}, as shown in Fig. 4.1 (a). To completely erode this excess and blind the detector, Eve needs to create a photocurrent I that can be approximated as

$$I = \frac{V_{\mathrm{ex}}^{0}}{R_{\mathrm{bias}} + R_{\mathrm{apd}} + R_{\mathrm{s}}/2}, \tag{4.1}$$

where R_{bias}, R_{apd} and R_{s} are the resistance values for the biasing resistor, the APD itself and the sensing resistor, respectively. In a usual setup, $R_{\mathrm{bias}} = 0$ and the current is determined mainly by the value of R_{apd}. Its typical value is on the order of 1 mA, see Fig. 4.1 (b). This large current, together with the gain modulation effect by the

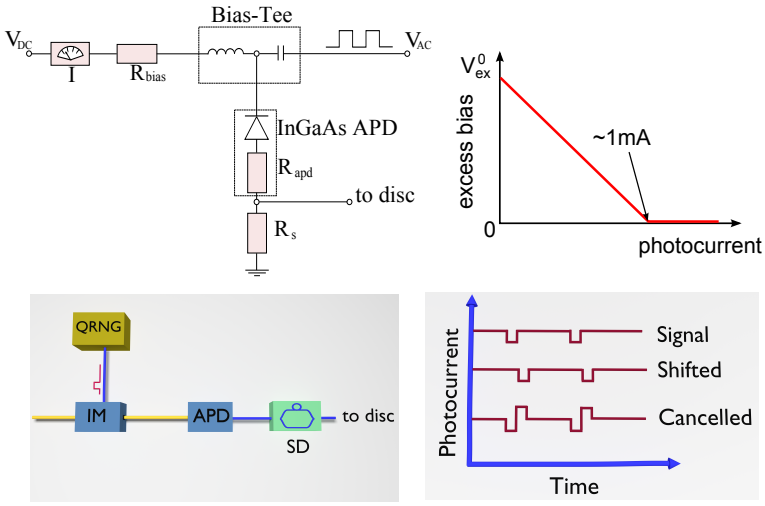


Fig. 4.1 **Outline of blinding and its countermeasure** *(a) Schematic of a biasing scheme for a gated APD. V_{DC} : DC bias component; V_{AC}: AC bias component; R_{bias}: biasing resistor; R_{apd}: APD internal resistance; R_s: sensing resistor. (b) Reduction in the excess bias due to photocurrent. (c) Schematic of the measure against blinding. IM: intensity modulator; QRNG: quantum random number generator; SD: Self-Differencer. (d) Effect of the intensity modulation on the SD photocurrent in presence of bright light inputted by Eve.*

detector gating, has previously enabled gated-APDs to avoid the blinding attack when their discrimination levels are appropriately set [161].

Here we propose a different measure, schematically shown in Fig. 4.1 (c). We insert an IM, driven by a quantum random number generator (QRNG), in front of the optical fibre input of the APD detector and an SD circuit after its electrical signal output. The SD circuit splits the APD output into two equal components, delays one of them, and then combines the two signals differentially, see Fig. 4.1 (d). The positive peaks of the resulting photocurrent can then be detected by the discrimination electronics.

The IM acts as an optical shutter and stops any incoming light for a short duration at random times. Under normal conditions, *i.e.*, in the absence of Eve, this would cause a decrease in the counts seen by Bob every time the IM is activated. Correspondingly, the resulting avalanche current would exhibit a waveform containing a positive current peak followed by a negative dip. On the contrary, if Eve sends her blinding pulses into Bob's module, the IM's activation would increase the counts seen by Bob, due to the SD effect, and the resulting photocurrent would exhibit a negative current dip followed by a positive peak. Because this outcome is distinctively different from that under normal conditions, it represents a clear signature of Eve's presence.

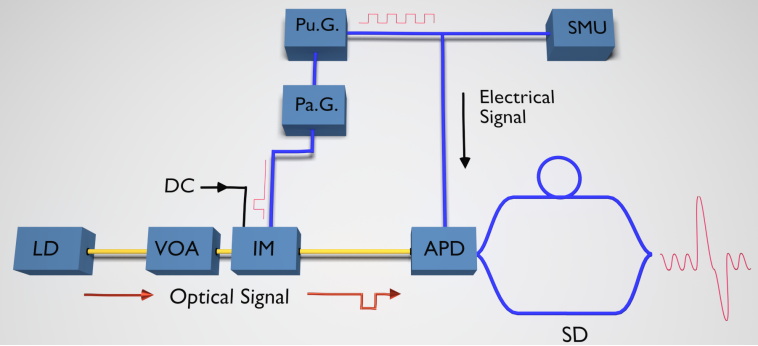


Fig. 4.2 **Experimental setup to investigate intensity modulation as a countermeasure against blinding**. *Pu.G.: Pulse Generator; Pa.G.: Pattern Generator; SMU: Source Measure Unit; LD: Laser Diode; VOA: Variable Optical Attenuator; IM: Intensity Modulator; APD: Avalanche Photodiode; SD: Self-Differencer.*

Even without correlating Bob's counts to the IM's activation times, the presence of the IM and SD circuitry make it possible to restore the APD's count rate and prevent its blinding. This is a simple consequence of the fact that, irrespective of the polarity of the photocurrent, the positive peak is always well above the detector's discrimination level, for a detector that has been correctly set up. So, for simplicity, we decided to not take advantage in this work of the "fine-grained" signatures based on correlating the counts with the IM or based on the avalanche's polarity and focus rather on the "coarse-grained" signature represented by the APD's counts. The analysis of the whole statistics available to Bob is left for future studies and can only reinforce the results presented here.

4.5 Experimental setup

To investigate the efficacy of the proposed measure, we modify the experimental setup from Chapter 2, shown in Fig. 4.2, which includes an IM and removes the bias resistor. Unless otherwise stated, the experimental condition are as before.

We use two variable optical attenuators (denoted as a single VOA in Fig. 4.2) to provide a 120 dB intensity variation range and a $LiNbO_3$ intensity modulator driven by a pattern generator to modulate the optical power.

We note that under this operating condition, specifically an appropriately chosen discrimination level of 18mV and no bias resistor, it is not possible for Eve to blind the detector using continuous-wave illumination because the increasing APD capacitive response is sufficient to counter Eve's blinding effort as shown in Chapter 2 and [184].

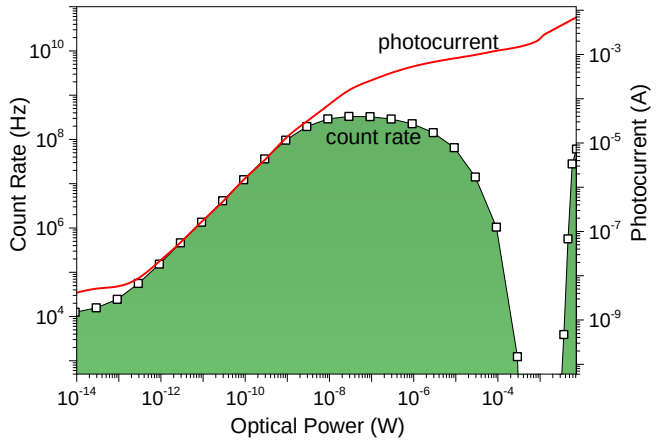


Fig. 4.3 **Blinding of an inappropriately operated APD** *The detector count rate in the case of an inappropriately high discrimination level and associated photocurrent as a function of the incident optical power. Count rate and photocurrent can be simultaneously measured and pose stringent constraints on Eve's actions.*

4.6 Effect of the intensity modulation on the count rate

We first demonstrate once more the experimental condition under which the SD-APD can be blinded (previously shown in Fig. 3.2). By deliberately setting the discrimination level inappropriately high, at 26 mV, we measure the count rate of the SD-APD as a function of incident optical power measured directly after the IM. Here, the RF input to the IM is disabled and its DC bias is adjusted to have a maximum transmission. Figure 4.3 shows the count rate and photocurrent as a function of the incident optical power. The detector exhibits a blinding gap between 300 μW and 3 mW, within which the detector count rate falls to zero. Such a blinding gap enables Eve to gain complete control of the detector. The photocurrent follows the count rate and grows linearly before the count rate saturation, and then grows sub-linearly (100 nW – 1μW) before becoming quasi-linear with the incident optical power ($> 1\mu$W). In the blinding gap, the photocurrent is measured to exceed 1 mA.

Such a large photocurrent offers an opportunity to close the blinding gap by modulating the intensity of the attacking signal. As illustrated earlier with Fig. 4.1 (d), intensity modulation creates a dip in the photocurrent. The SD circuit converts each dip to a positive peak which can trigger the detector discrimination circuit when there is sufficient modulation depth. A random pattern produces photocurrent dips at a rate that is 1/4 of the signal clock rate. For simplicity we simulate this rate in our experiment by applying an RF signal to the IM using a repetitive modulation pattern "0001", which we label as "1/4" modulation. We set the RF amplitude to 4 V (V_π),

achieving half-wave modulation and an intensity extinction ratio of 23 dB. This pattern carves a 1 ns hole for every 4 ns duration in the attacking light intensity.

Using the ill-set discrimination level of 26 mV, we measure the count rate versus the incident optical power with the result shown as black squares in Fig. 4.4 (a). The intensity modulation causes distinctively different count rate behaviour for higher optical power when compared with the case without intensity modulation (open squares). The count rate stays above 250 MHz from 100 nW to 7.5 mW, without any sign of it falling. Despite the high discrimination level, the IM successfully removes the former SD-APD's blinding gap.

We attribute the closure of the blinding gap to the applied intensity modulation. To illustrate this, we compare two SD-APD output waveforms recorded using a 16 GHz oscilloscope under vastly different optical powers. In the single photon counting regime, the APD produces a positive, current spike and therefore its SD output becomes a positive spike followed by its negative copy 1 ns afterwards, see waveform 1 in Fig. 4.4 (b). With an optical power of 1 mW, the SD-APD output waveform reverses its polarity (waveform 2) because the intensity modulation carves a hole in the photocurrent, instead of a current spike for a single-photon induced avalanche. The signal level is about 9 times as strong as the single-photon induced avalanche, and can therefore overcome the detector discrimination level. For the case of 1/4 modulation, the count rate saturates close to 750 MHz, which can be explained by having two ripples after the main avalanche peak in Fig. 4.4 (b) overcoming the discrimination threshold as well.

Figure 4.4 (c) plots the signal level of the main positive peak extracted with in-built scope functionality induced by the IM as a function of incident optical power. Over the incident power spanning over 4 orders of magnitude between 0.7 μW and 7 mW, the IM induced signal has a significant margin to overcome the discrimination level, even though it was inappropriately set. At an optical power of 1 μW, where the count rate with no IM (open squares in Fig. 4.4 (a)) begins to fall, the signal level in Fig. 4.4 (c) is over 50 mV and continues to increase in amplitude to over 300 mV at an optical power of greater than 1 mW. Within the power range Eve needs for blinding, each intensity modulation is guaranteed to produce at least one detector count. This is in agreement with our experiment using sparser modulation patterns, as shown in Fig. 4.4 (a). A sparser modulation results in a proportionally lower bottom-out count rate in the blinding gap.

The significant margin in the signal level shown in Fig. 4.4 (c) offers room to relax the requirement on the IM's modulation contrast, thus minimising the loss that the IM would introduce. This would also be beneficial as the halfwave modulation requires

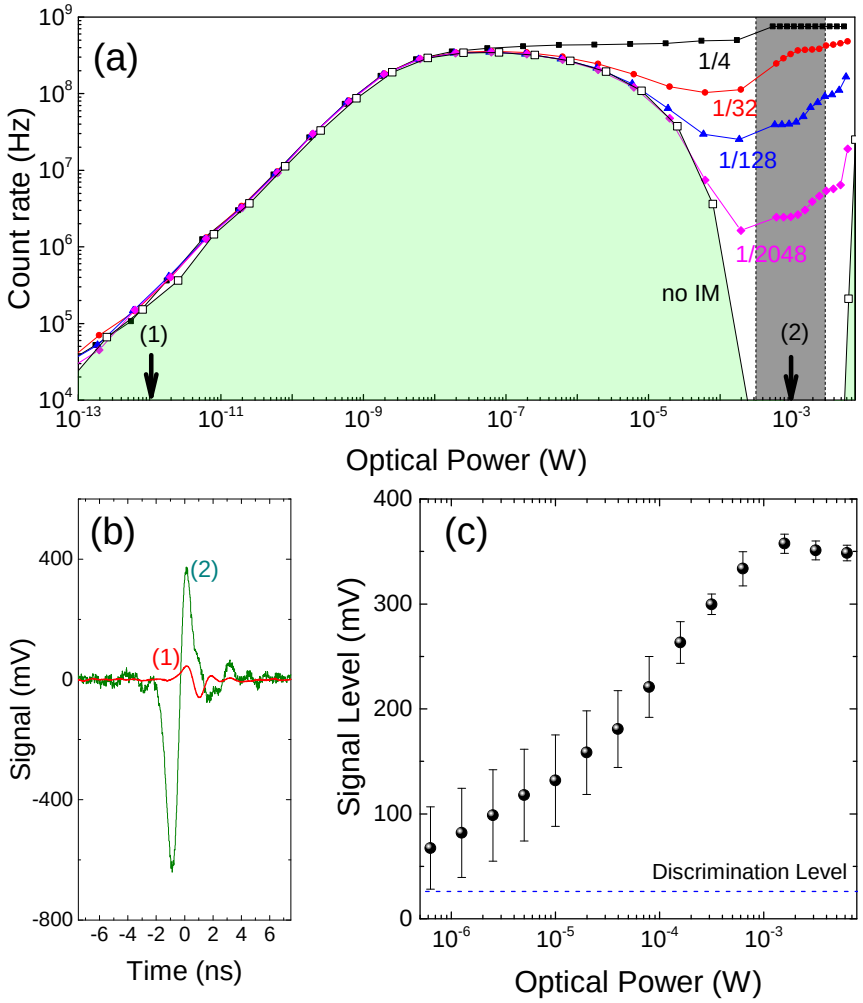


Fig. 4.4 **Effectiveness of the intensity modulator** *(a) APD count rates as a function of incident optical power with different modulations applied to the intensity modulator. An RF amplitude of 4 V is used to produce half-wave modulation and a modulation extinction ratio of 23 dB. (b) The SD output recorded by the oscilloscope at points (1) and (2) in (a) with the attacking laser being modulated by a "1/32" pattern. (c) Signal level of the main positive peak as a function of optical power.*

an RF voltage of 4 V, which is undesirably greater than the value of 3 V that is easily reachable with low cost and low power-consumption semiconductor integrated circuits. The DC is first set to maximum transmission such that the extinction is minimised, as shown in Fig. 4.5 (a). The arrival time of the modulated optical power is also optimised by adjusting the delay on the pulse generator driving the IM and maximising the amplitude of the corresponding APD waveform, as shown in Fig. 4.5 (b).

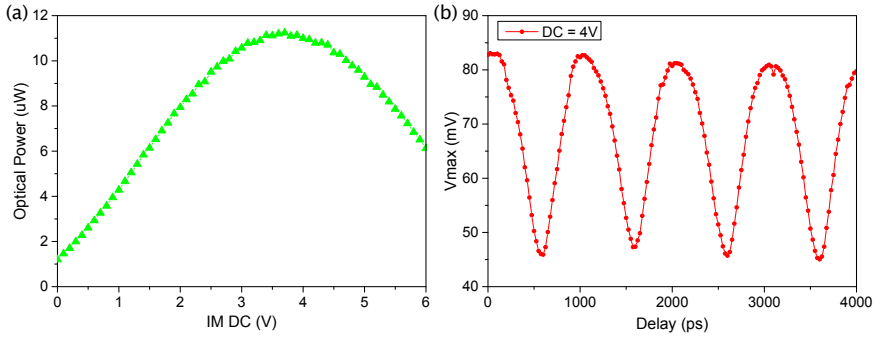


Fig. 4.5 **Calibrating the intensity modulator** *(a) Optical power as a function of IM DC with the RF signal turned off. (b) APD signal amplitude as a function of delay.*

With the IM calibrated, we determine the lowest modulation contrast by measuring the count rate probability as a function of the RF signal amplitude applied to the IM. Here, the modulation frequency is 1/128 of 1 GHz and the incident optical power is 1 mW. As shown in Fig. 4.6, a modulation signal with amplitude 0.3 V can always induce at least one detector count. More counts are possible due to the ripples in the output waveform also overcoming the discrimination threshold. This RF level corresponds to an intensity contrast of 0.06 dB, calculated using the equation [185]

$$contrast = 10\ \log\left\{\frac{1}{2}\left[1+\cos\left(\frac{V}{V_\pi}\pi\right)\right]\right\} \tag{4.2}$$

The number of counts increases above unity at a modulation amplitude higher than 1.5 V because the amplitude of the signal ripple (see Fig. 4.4 (b)) rises above the discrimination level.

4.7 Intensity modulation to prevent blinding

In this section we discuss how the IM represents a potential countermeasure to the blinding attack. We also neglect any artificial additions used to facilitate post-processing or software implemention, such as dead time, which may be exploited by Eve with a modified attack [186]. We assume that the IM is driven by a true random generator,

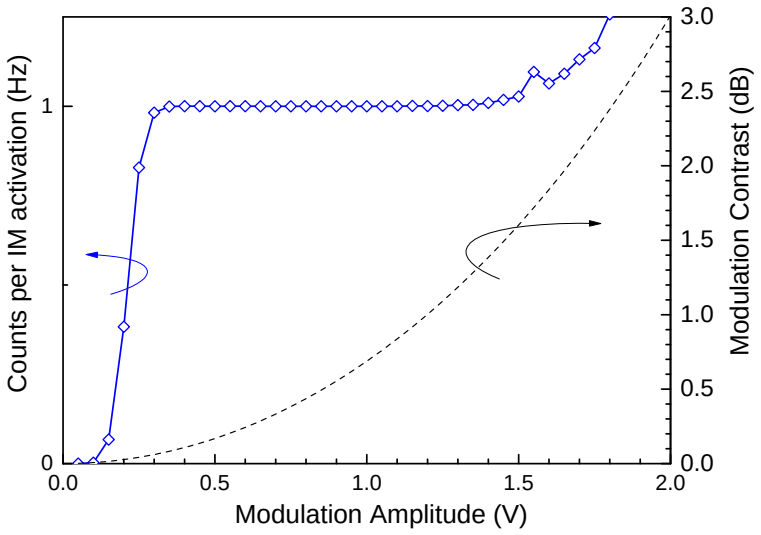


Fig. 4.6 **Required contrast to mitigate blinding.** *APD counts per IM activation and IM contrast as a function of the AC signal driving the IM, for a constant incident optical power of 1 mW and a modulation pattern 1/128. We note that the APD discrimination level is deliberately set too high (26 mV) to enable blinding when the IM is switched off.*

so Eve cannot deterministically predict the modulation effect and prepare her blinding pulses accordingly. In active basis selection schemes, as in the most commonly implemented BB84 protocol, Bob already contains a random number generator. This can be operated at twice the clock frequency and thereby provide random numbers for both basis selection and intensity modulation and thus reducing the complexity of the countermeasure. Removing the need for an additional random number generator therefore does not open additional side-channels.

We also consider a sufficient modulation depth to ensure a strong signal difference between modulated and unmodulated gates, which guarantees the occurrence of a detector count, as we have shown. The synchronisation of the IM pulses, as well as the differential delay of the SD circuit, must be carefully chosen such that the counts by IM activation fall within the acceptance time window of the QKD system. Finally, a spectral filter should be applied in the QKD receiver to limit Eve's choice of wavelength and ensure that the modulation effect on Eve's attacking signal takes place.

Whilst most intensity modulators are polarisation sensitive, we note that placing the IM directly before the detectors makes this irrelevant. In phase-encoded systems, such as in ref [19], the interferometer at Bob contains an electronic polarization controller (EPC) and a polarizing beamsplitter (PBS) which ensure that the polarization is fixed once it arrives at the detectors. For polarization encoded schemes, such as that investigated in [134], a PBS is also used, thereby ensuring the same effect. Therefore,

regardless of what polarization Eve might send into Bob, the received polarization at the detectors always remains the same.

The main security observation is that each IM-induced electrical signal overcomes the discrimination level and deterministically generates at least one detector count. These counts have equal probabilities of contributing a correct or incorrect bit in the sifted key, thus generating an overall 50% QBER. Therefore we can choose the probability to activate the IM, P_{IM}, such that the resulting QBER in the presence of Eve exceeds the security tolerance of the protocol. If this happens, the protocol is aborted and no insecure key is distilled.

To decide the correct value for P_{IM}, let us consider the BB84 protocol [9], which features a security tolerance of 11%. Suppose first that $P_{IM} = 25\%$. In this case, we have a guarantee that if Eve always launches her attack, Bob will see at least 1 click in 4 input pulses, which would cause a QBER, Q_b, equal to or larger than 12.5%. In this case the key rate is zero, $R(Q_b) = 0$. If Eve works in "burst-mode", she cannot do better than in the previous scenario. On the N preparations effected by Alice, she could intercept-and-resend N_b consecutive blinding signals in bursts and mount her attack only on these bursts, while blocking the remaining $N - N_b$ quantum signals. Even in this case, the IM would guarantee the final QBER to be above 12.5%, causing zero key rate. Moreover, at the beginning of the train of blinding pulses prepared by Eve, the SD effect would cause one additional count in Bob's detectors, making this scenario more favourable to the legitimate users. This analysis is somewhat naive and can be considered overly conservative, possibly needlessly reducing the secure key rate. Since Bob knows exactly when he activates the IM, he could estimate two different QBERs, each corresponding to the IM being enabled or not. Therefore, even if $P_{IM} = 0.001\%$, Bob would still measure the QBER with the IM enabled to be 50%.

On the other hand, assuming Bob has a rather crude QKD system and is unable to distinguish between cases with the IM being enabled or not, Eve could let a fraction of Alice's signals pass undisturbed. In this case, Eve gets no information on the undisturbed signals, but the resulting QBER would be smaller than the protocol's tolerance and the users would not abort the transmission. For simplicity, let us divide them into three scenarios:

① Eve does not interact with Alice's pulses. Therefore Alice and Bob see a QBER that does not include any interference from Eve and is below 11%.

② Eve interacts with every pulse Alice sends, thus causing a QBER that is greater than 11%. If $P_{IM} = 25\%$, then the QBER would be 12.5%, as discussed.

③ An average of the previous scenarios, so the overall QBER is an average as well, and smaller than 11%.

These scenarios are illustrated in the top section of Fig. 4.7. Although the QBER is below 11% in scenario ③, this case is still secure due to the fact that the key rate is a convex function of the QBER (see e.g. [10, 187]) and, conversely, Eve's information is a concave function of the QBER, as shown in the bottom section of Fig. 4.7. Suppose that C_1 and C_2 (Q_1 and Q_2) are the count rates (QBERs) pertaining to undisturbed and blinding pulses, respectively. Then the average QBER seen by the users is $Q_3 = \frac{C_1Q_1+C_2Q_2}{C_1+C_2}$. The convexity of the key rate and the fact that $R(Q_2) = 0$ imply that

$$R(Q_3) \leq R(Q_1) + R(Q_2) = R(Q_1), \tag{4.3}$$

where $R(Q_1)$ and $R(Q_2)$ are the key rates from separate undisturbed and blinding pulses, respectively. Eq. (4.3) shows that there is at least a fraction $R(Q_1)$ of secure bits in the users' signals. This comes from the fact that $R(Q_1)$ is associated with the undisturbed pulses. In the real case, the users measure Q_3 and distill a secure fraction $R(Q_3)$, rather than measuring Q_1 and Q_2 separately. This, by virtue of Eq. (4.3), is a pessimistic estimate of the fraction of secure bits in the sample, hence the protocol is secure. Looking at Fig. 4.7 again, this is because Eve's information is actually given by I_m, but since Alice and Bob don't examine scenarios ① and ② separately, they calculate Eve's information to be I_3, thereby overestimating it and carrying out more privacy amplification than required. This guarantees that Eve's information is always zero.

4.8 Intensity modulation for 'free'

We note that some QKD systems may already contain the architecture for introducing this modulation without the need of additional components. We consider a receiver configuration used in the T12 protocol, a type of phase-encoded QKD protocol [19] in Fig. 4.8. In this protocol, Alice uses an unbalanced Mach-Zehnder Interferometer (MZI) to encode her qubits on her weak coherent pulses and an intensity modulator for performing the decoy state method. Bob then uses a matching MZI for decoding the pulses, with a polarisation controller (PC) beforehand to ensure the light is split equally at the PBS such that interference occurs at the final beamsplitter (BS).

In this set-up, Eve instead aims to send all of her blinding power down one arm of the MZI such that no interference occurs at the final beamsplitter and the optical power is split equally between the two detectors, thus blinding them. However, as the first

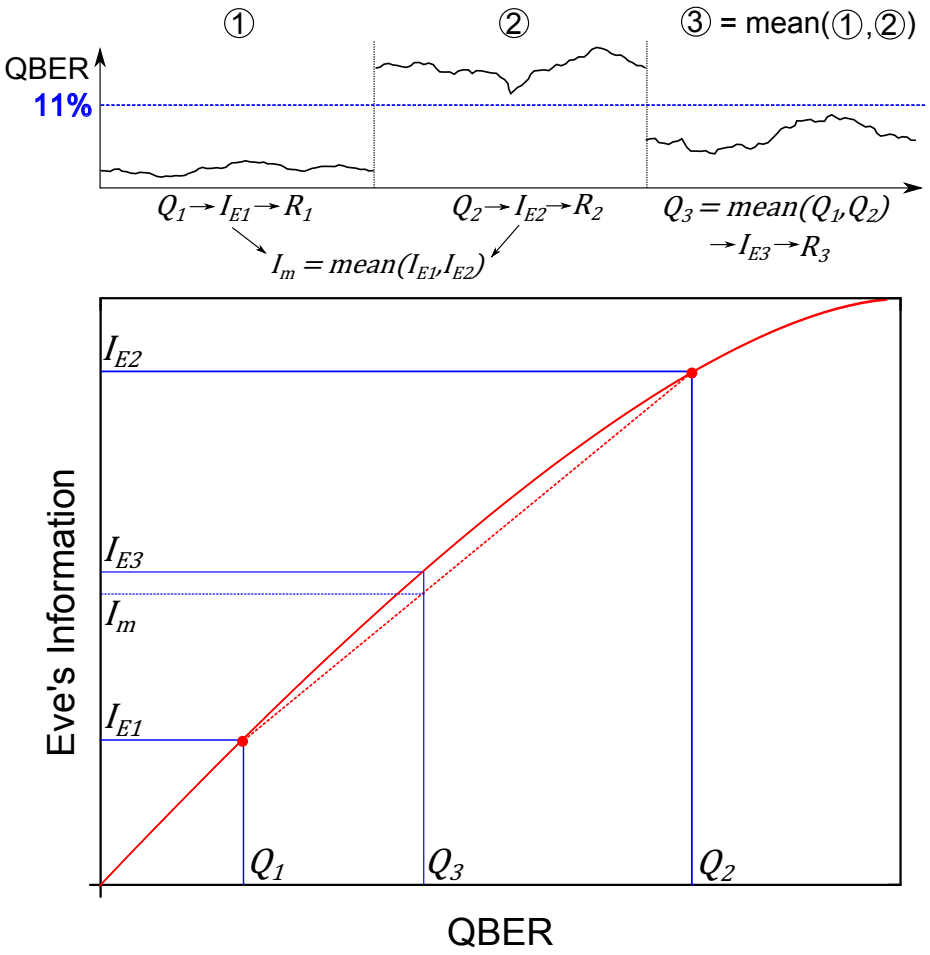


Fig. 4.7 **Eve’s information** *Illustrated explanation of the relationship between Eve’s information and the QBER. The top section of the figure indicates the QBER in three scenarios, where Eve doesn’t mount her attack, always mounts it and the average of the two, respectively. For each QBER, Eve’s information and the subsequent secure key rate can be determined by the users. The bottom figure shows her information as a function of the QBER. It demonstrates that if Alice and Bob only pay attention to the overall average QBER and infer Eve’s information from this, they in fact overestimate her knowledge, which is more accurately given by an average of Eve’s information extracted from the two separate QBERs,* Q_1 *and* Q_2.

polarizing beamsplitter (PBS) has a finite extinction ratio, some light will always leak down the other arm. When Bob applies his phase modulation to choose his basis, he is introducing a phase difference between the two arms and in the scenario where Eve sends bright CW light into the MZI this has an analogous effect to using an intensity modulator.

To investigate this, we place the MZI depicted in Fig. 4.8 between the IM and APD shown in Fig. 4.2. In this instance, we initially operate the IM differently, for the purpose of pulse carving our CW to simulate a pulsed laser. This was done to so that calibration and demonstration of our countermeasure to blinding could be performed without disturbing the set-up and the same laser could be used for both steps. Initially, the output of the IM was connected to a power meter. A 1/64 modulation was used for calibration and the optical power as a function of the IM DC was minimised so that the background was kept as low as possible. After this step, the IM was then connected to the PC which was in turn connected to the MZI, one of whose outputs was connected to a fast photodiode plugged into the oscilloscope.

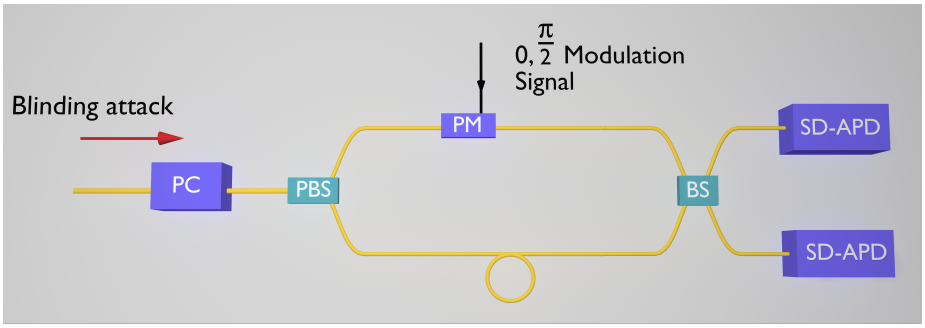


Fig. 4.8 **Bob's receiver** *Configuration of Bob's decoding apparatus used in the T12 protocol. PC: polarisation controller; PBS: polarising beamsplitter; PM: phase modulator; BS: beamsplitter; SD-APD: self-differencing avalanche photodiode.*

The polarisation is calibrated using the PC such that the majority of the optical power goes down one arm, as shown in Fig. 4.9 by the blue curve where only one pulse is visible and its height has been maximised. The red curve shows an uncalibrated situation for comparison, where two pulses are visible. This situation is then verified by varying the DC to the phase modulator (PM) in the MZI and monitoring the pulses. If the majority of light is travelling down one arm, then adjusting the relative phase between the two arms of the MZI would make no difference as no visible interference is occurring at the BS. Therefore, if changing the DC to the PM has no effect, this confirms the input light has been properly calibrated.

We therefore measure the count rates of one of the detectors when modulation is applied with a $1/16$ modulation rate, as is typical for the T12 protocol, shown in

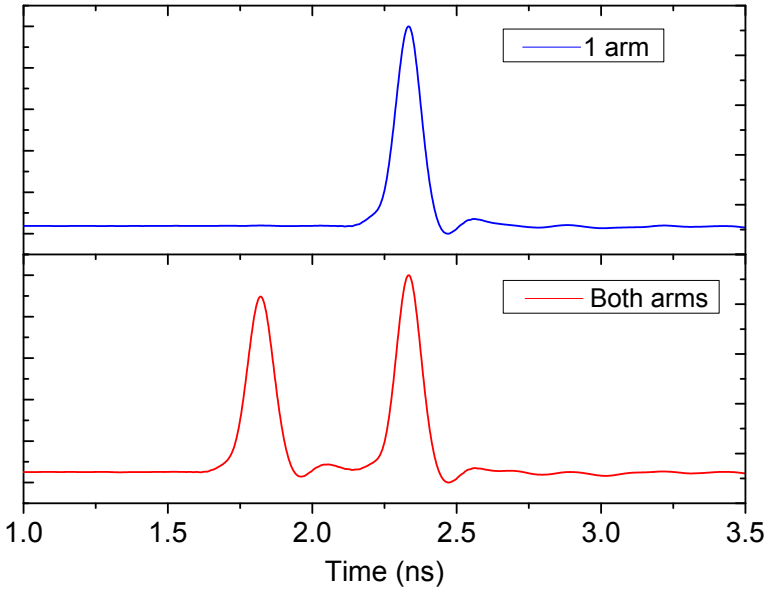


Fig. 4.9 **Mach-Zehnder interferometer calibration** *Oscilloscope traces taken at one of the output ports where the polarisation at the polarisation controller in Fig. 4.8 is adjusted to control how the light propagates through the interferometer. The top case denotes the majority travelling down one arm, the desirable case for Eve, whereas the bottom part shows a non-calibrated set-up.*

Fig. 4.10 (a). We find that this causes a similar recovery to that observed with the IM and this is confirmed by examination of the resultant waveform, see Fig. 4.10 (b), suggesting that, in fact, the power is not all travelling down one arm due to the aforementioned imperfect extinction ratio of the PBS. We note, however, that this is limited to the case where Eve uses a CW laser. By using a pulsed laser, Eve can avoid interference at the final BS and thus bypass this countermeasure.

4.9 Summary and Discussion

In conclusion, we have devised and experimentally demonstrated a new technique to mitigate detector blinding. By using an intensity modulator and an SD circuit, we modulated the incoming light to create uneven avalanches for the case of strong input light. Significantly, whilst this protects the detector from Eve it only introduces a small intrinsic attenuation of Alice's signal. We showed that a modulation depth of 0.06 dB is sufficient to prevent an SD detector from being blinded. In our experimental test, we adopted a continuous-wave laser. A pulsed laser would be no more effective at blinding an SD detector as it creates more intensity fluctuations, to which the detector is very sensitive. Although intensity modulation to prevent Eve's faked-state attack has been previously addressed in the literature [142], this was concerned with controlling

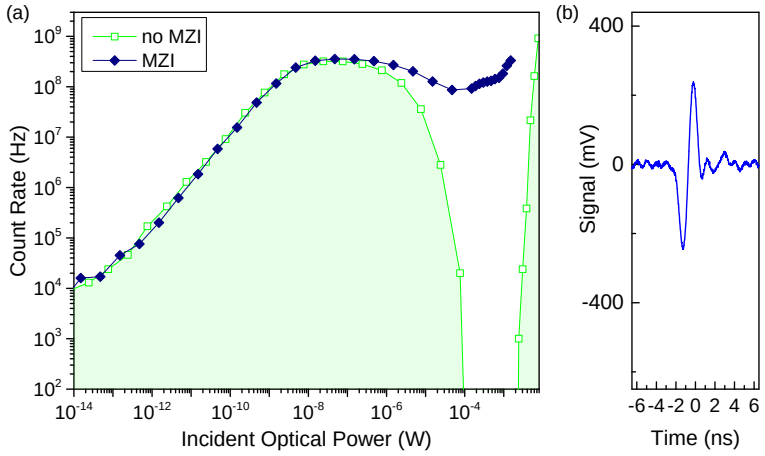


Fig. 4.10 **Inherent countermeasure against CW blinding** *(a) APD count rates as a function of optical power in the presence and absence of the MZI. (b) an example APD waveform taken using with the MZI in use and with an optical power that would cause the APD to be blind otherwise.*

an *already blinded* detector. Our approach, on the contrary, includes a SD circuit to prevent blinding in the first place and thus eliminate the possibility of a faked-state attack at the root.

The proposed IM measure entails a considerable extrinsic loss penalty of around 2.5–5 dB, arising from imperfect intensity modulators based on $LiNbO_3$ and will therefore negatively impact the secure key rate. The loss associated with the product of the modulation rate of 1/4 and extinction ratio of 0.06 dB is comparatively negligible, hence the key rate in the presence of modulation would be 0.315 times the unmodulated key rate and the distance would be shortened by 25 km, assuming a maximum insertion loss of 5 dB. Although QKD systems typically have two or more detectors, placing an intensity modulator in front of only one would be sufficient to demonstrate the presence of Eve. We note that existing modulators were designed to achieve high modulation depth which requires a lengthy crystal waveguide for electro-optical interaction. With a reduced modulation depth, the insertion loss can be made significantly smaller, thereby alleviating the loss penalty. Although intensity modulators are typically polarization sensitive, Eve cannot mount an attack such that she simply sends light of a polarization which does not experience modulation. This is because the detectors in a QKD system always see a fixed polarization, whether in phase-encoded schemes such as [188], which contain an electronic polarization controller followed by a polarizing beamsplitter (PBS) or in polarisation-encoded schemes, such as in [134], which also have PBSs before the detectors. The use of an IM also requires a random number generator (RNG). Since Bob typically already has an RNG for the purpose of active

basis selection, he can use the same RNG operated at twice the clock rate for the IM, which would not open additional side-channels.

Although the two techniques of mitigating the blinding attack have been shown, namely with best-practice operation and the use of an IM, the faked state attack in general can still pose a threat. Eve can choose not to use a blinding attack and instead carefully adjust the arrival time of her trigger pulse in order to control Bob's detectors, which is the focus of the following chapter.

Chapter 5

After-gate attack

5.1 Introduction

The previous two chapters have focused on attempts to mount the faked-state attack by first blinding the APD so it is insensitive to single photons. However, a more dangerous attack exists in the form of the faint-after gate attack, where the avalanche photodiode (APD) maintains its single-photon sensitivity, as no blinding laser is used and it is therefore more difficult to provide a countermeasure or detect Eve's presence. This chapter will explore the noise exhibited as delayed detection events found in fast-gated detectors that could be used as a measure against the faint-after gate attack.

5.2 The material interface

Gated APDs have been shown to exhibit a short exponential decay in detection events occurring in the gates following the illuminated gate when biased at high gating frequencies (i.e. on the order of GHz) [68, 128, 189–192].

The explanation of this phenomenon is incompatible with afterpulses which are additional avalanches occurring after, and correlated with, photon detection. These afterpulses take place as a result of deep traps in the multiplication region and have decays on the order of several nanoseconds or greater [1, 104, 105]. The observed short decay is, however, consistent with carriers being delayed and later released through thermionic emission at the potential barrier arising out of the material interface occurring in InGaAs/InP devices manufactured according to the separate absorption and multiplication structure [81, 91]. Recapping from chapter 2, in such a structure, outlined in Fig 5.1, incoming photons are absorbed in the InGaAs region where electron-hole pairs are generated and subsequently separated by the low electric

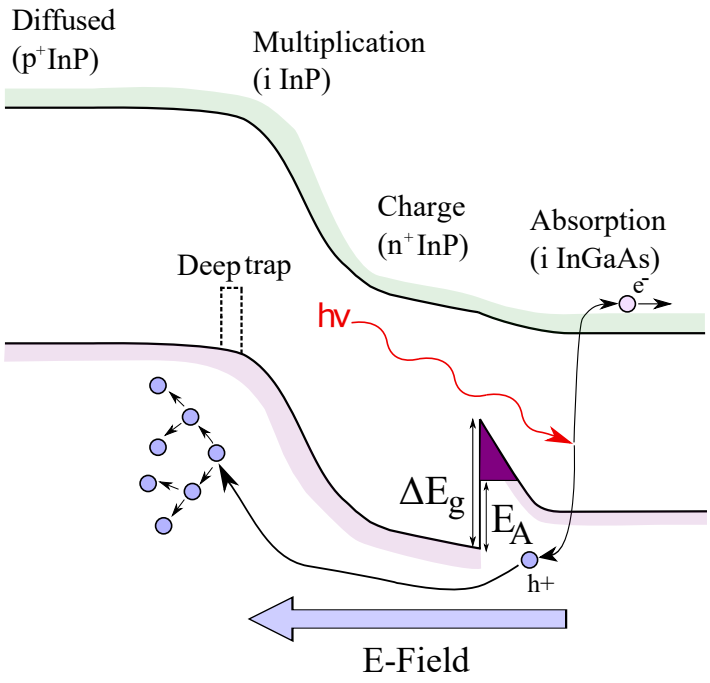


Fig. 5.1 **APD structure** *Typical band diagram of separate absorption, charge and multiplication structure of an InGaAs/InP APD, where E_g is the band gap offset and E_A is the effective barrier height.*

field in this region. Due to its higher ionisation coefficient in InP [89, 90], the hole is then swept towards the InP multiplication region. In order to reach the InP multiplication region, the hole needs to overcome the potential barrier that arises from the aforementioned valence-band mismatch [193]. The ability of the hole to surpass this is directly related to device characteristics such as detection efficiency and timing response [194]. Due to this relationship, it is reasonable to conclude that the hole traverse time is significantly shorter than 1 ns because sub-nanosecond gated-APDs still show detection efficiencies as high as 55% [68]. If the decay time were longer than 1 ns, then fewer than half of the generated carriers would overcome the barrier and the detection efficiency would not be able to exceed 50%. On overcoming the barrier, the hole arrives at the multiplication region where it undergoes impact ionisation and generates many more carriers, known as an avalanche, and some of these carriers are then trapped in deep levels in this region [104, 127]. A macroscopically detectable current is then created from this carrier multiplication or avalanche, allowing it to be electronically registered.

In order to mitigate the effect of the potential barrier and allow carriers to more easily traverse it, the concept of a grading layer was introduced [92]. This involves the placement of a small InGaAsP layer between the InGaAs absorption and InP charge layers. As the name suggests, this ‘grades’ the discontinuity that arises from

the valence band mismatches of the two materials and facilitates the transport of the carriers within the device. The smoother the transition, the faster the response times of the device and likely the smaller the effect of noise as a result of carrier trapping at the interface, although a relationship between the two has not been explicitly explored in the literature.

Until recently, delayed detection events as a result of this potential barrier have been considered explicitly only in terms of a drawback. However, it can act as a positive as it could be used to mitigate a type of attack available to Eve, the faint-after gate attack, explored in the following section.

5.3 After-gate attack

In many demonstrations of the faked-state attack, Eve first blinds the detector so that it is insensitive to single photons before mounting her attack. Performing it in this way makes it more likely that she will leave a strong signature of her presence. As such, it is desirable for her to remove the need for this step and employ the after-gate attack, first proposed and demonstrated in [186]. The authors focused on the Clavis2 system from IDQuantique and were able to mount attacks that introduced a QBER below 11%. Whilst this satisfies the condition of Alice and Bob not aborting their exchange, she still introduces fingerprints of her presence, for example in a raised afterpulse rate or the introduction of clicks in Bob's detectors that would not occur due to the dead-time of the system. Furthermore, since reasonably bright pulses were used, a non-avalanche based watchdog detector at Bob could be used to detect Eve. In order to make things clear and distinguish this from the faint after-gate attack, this will be referred to as the *bright* after-gate attack (although we later show in section 5.5.1 these are likely extensions of one another).

Later, the same group proposed a similar technique to strengthen Eve's strategy, known as the *faint* after-gate attack (so-called to distinguish it from the bright after-gate attack in [186]). As before, Eve measures the photons sent by the transmitter, Alice, with a copy of Bob's apparatus. She then sends her own pulses to Bob which are only detected if he chooses the same measurement basis as Eve, else he registers nothing. In this way, after Alice and Bob exchange basis information, Eve has a string that is perfectly correlated with that held by Alice and Bob. The aim for Eve is thus to send a pulse which at full power registers a click with detection probability of 1 and at half power (corresponding to incompatible bases), registers a click with probability 0. More generally, when the probability at full power exceeds twice that of half power in this manner, the relationship is said to be 'superlinear'. If Eve sends strong pulses

towards the end of Bob's APD gate, she can maximise and minimise these probabilities such that she learns most of the key and also generates a sufficiently low QBER to go undetected. The original demonstration [137] involved sending pulses of moderately high flux (~ 40 photons/pulse) at the end of the APD gate.

By obtaining the detection probability at full power and half power, it is possible to derive the resultant QBER using the following equation from [137]:

$$QBER = \frac{2p_h - p_h^2}{2p_f + 2(2p_h - p_h^2)}, \tag{5.1}$$

where p_f is the detection probability at full power and p_h is the detection probability at half power. Note that this equation neglects any errors arising due to dark counts or afterpulsing and thus only focuses on the detection probability at the target gate. If the QBER drops below approximately 21%, this indicates superlinearity as $p_f > 2p_h$.

The original demonstration of the faint after-gate attack did not produce a QBER below 11% with any of the fluxes used, although superlinearity was observed. The authors attributed this partly due to the large temporal width of the laser used in their study. More recently, the attack was demonstrated on a number of different detectors with a range of gating frequencies up to 1 GHz, with QBERs as low as 0.31% [195], although a convincing countermeasure was not presented, highlighting that this is still an open problem for QKD systems.

We therefore sought to investigate delayed detection events with the aim of answering two longstanding QKD questions. Firstly, what is the origin of the short decay in fast-gated APDs and can it be characterised? Secondly, can this short decay be used as a measure against the faint after-gate attack?

5.4 Characterisation of the fast decay

To examine the short decay in fast-gated detectors, we use a setup similar to that outlined in [95]. We initially approached the characterisation of the interface in a similar fashion to [196]. By measuring the single-photon detection efficiency as a function of the inverse of the temperature and plotting in an Arrhenius configuration, the barrier height could be extracted as the gradient is equal to ε_b/k_BT [193]. Here, we optically excite an APD at the start of a gate, as shown in Fig. 5.2. When a hole fails to overcome the potential barrier within Gate 1, it will have a finite probability to overcome the barrier and initiate a macroscopic avalanche in subsequent gates within several nanoseconds.

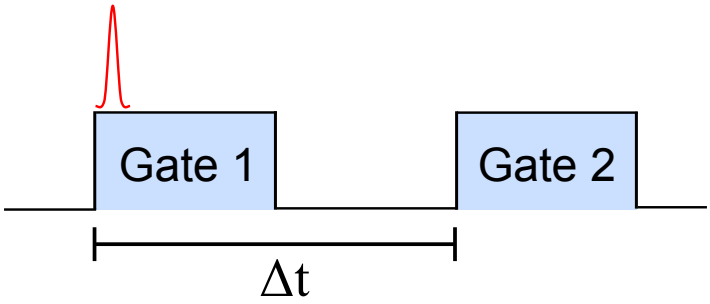


Fig. 5.2 **Illustration of APD gating scheme** *Charges are generated at the start of Gate 1, where the laser is timed to arrive, and experience an exponential decay between the two gates. The proportion of charges leftover at Gate 2 is related to the decay constant which is in turn related to the activation energy given by the barrier height, E_A*

In order to probe the after-gate attack with conditions that are most favourable to Eve, we employed a passively modelocked laser with a repetition frequency of 20 MHz and temporal pulse width of 3 ps. Due to the passive nature of the laser, this required significant adjustment of the electronics to ensure the APD gates and laser pulses were synchronised. An outline of the setup used to provide a synchronised 1 GHz AC signal to the APD is given in Fig. 5.3

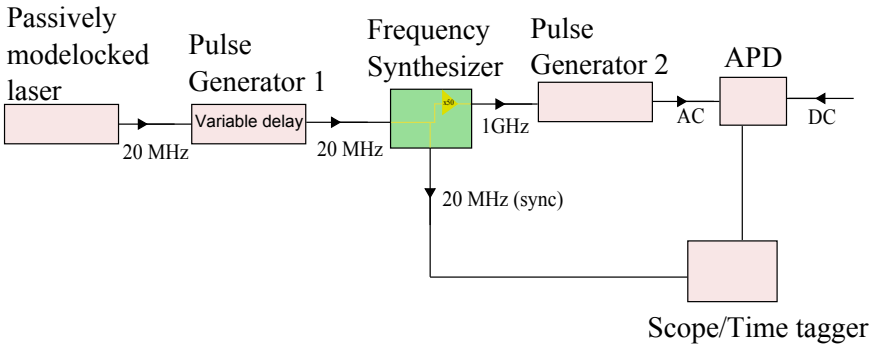


Fig. 5.3 **Laser and APD synchronisation scheme** *An outline of the set-up required to synchronise the passively modelocked laser with the APD gating apparatus. A jitter-cleaning evaluation board was needed to multiply the 20 MHz signal to 1 GHz for driving the APD*

Avalanches were discriminated using the self-differencer board comparator and an appropriate discrimination level was chosen according to the procedure from Chapter 3 and [184, 197]. The avalanches were then counted with an electronic time-tagger whose results were analysed using a LabView programme.

When extracting the APD characteristics of detection efficiency, dark count rate and afterpulsing, a 50 ns long histogram is obtained under dark conditions and when

the APD is illuminated with a flux of $\mu = 0.1$ photons per pulse. The detection efficiency, η, is calculated using the following equation

$$\eta = \frac{1}{\mu} ln\left(\frac{1 - P_d}{1 - \frac{R}{f_l}}\right) \tag{5.2}$$

where μ is the photon flux per pulse, P_d is the dark count probability (the count rate under dark conditions divided by the gating frequency of 1 GHz), R is the count rate in the illuminated bin of the histogram and f_l is the repetition frequency of the laser, in this case 20 MHz.

The choice of biasing conditions requires careful consideration as the breakdown voltage is dependent on the APD temperature. We measure this and find that the breakdown voltage increases at a rate of roughly 0.1V/°C, as shown in Fig. 5.4, which is consistent with the literature [39]. Therefore, although good experimental practice might suggest that the conditions be kept constant, this would produce an opposite trend to that expected, since the excess bias would simply decrease with increasing temperature as the breakdown voltage increases (as shown in [119] for example). The aim is therefore to keep the conditions within the device as consistent as possible.

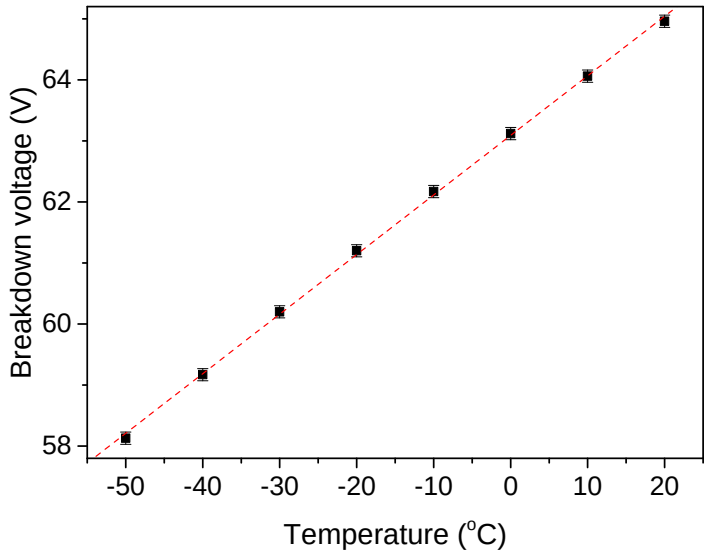


Fig. 5.4 **Breakdown voltage temperature dependence** *A linear fit of the measured points yields a relationship of approximately 0.1V/°C.*

The device is characterised to have a single photon detection efficiency of 28% and an afterpulsing probability of 4% at room temperature. Here, the optical flux is kept at 0.1 photon/pulse and its delay is adjusted by shifting the APD gates on the pulse generator to maximise the efficiency. A maximum efficiency corresponds to the photon

arrival at the beginning of a gate (Fig. 5.2), which allows an avalanche sufficient time to grow so as to surpass the discrimination level. A proportion of carriers remain trapped at the material interface due to the presence of the interface potential barrier and are subsequently released in the following gate.

Figure 5.5 (a) shows a typical photon detection histogram under such illumination conditions. The illuminated gate gives a pronounced peak arising from single photon detections. Immediately after this peak, the count rate experiences a fast decay before reaching an approximately flat background at the fifth gate. The flat background is attributed to detector dark and afterpulsing counts. The elevated count rates at Gates 2-4 cannot be attributed to detector afterpulsing because the time-tagger has a dead time of 50 ns. Moreover, the sub-nanosecond decay time is orders of magnitude faster than typical lifetimes of deep traps that are responsible for afterpulsing. We attribute the elevated count rates at these gates to delayed photon detection caused by hole trapping at the absorption/multiplication interface.

The time-decay was automatically calculated by first subtracting the background that arises from 'conventional' afterpulsing. As these are thought to arise from deep traps in the multiplication region and have longer decay constants, taking the average of the count rates in the gates preceding the illuminated gate gives a good indication of the afterpulse count rate. After subtraction, only delayed detections arising from the material interface should be left, allowing for an accurate calculation of the corresponding decay constant. The decay constant is then taken using the natural logarithm of the ratio between the count rates in Gates 1 and 3 (Gate 2 is ignored to ensure the self-differencer does not affect the result).

By examining the second bin of the histogram in Fig. 5.5 (a) (which corresponds to Gate 2 in Fig. 5.2), we already have a clear indication of the interface playing a role. If afterpulsing were the sole source of trapping resulting in delayed detection in this bin, due to self-differencing cancellation, this bin would be heavily suppressed. The imposed deadtime of 50 ns also has the same effect, meaning clicks registered in bin 2 are uncorrelated with those occurring in bin 1, so they cannot occur as a result of afterpulses. The observed short decay of 289 ps in the histogram must therefore arise from a separate source of trapping, namely the material interface.

Plotting the lifetimes extracted from Fig. 5.5 (a) at different temperatures in an Arrhenius configuration allows for the extraction of the effective barrier height at the material interface [193], shown in Fig. 5.5 (b), where the gradient is equal to ε_b/k_BT. We note that the values of activation energies and the trend of higher excess biases resulting in overall shorter lifetimes, and consequently lower activation energies, are consistent with the literature [193, 196]. This implies that carriers with shorter decays

of several hundred picoseconds are dominated by trapping at the heterointerface when the APD is illuminated with fluxes of the order of single photons.

Whilst the technique used to obtain Fig. 5.5(b) contains similarities to those used in [196], they are not identical. Ideally, the values of activation energies would be checked using those techniques, but we were unable to cool the APDs to the required temperature. Therefore, although the values and trends appear to bear agreement to the literature, we are hesitant to definitely conclude the activation energy at the interface has been measured. Indeed, it is likely that traps of varying depth exist in the multiplication region, and these could also display similar results. Although this suggests that further study is needed, the presence of the delayed detections themselves is beyond doubt and they can still be utilised to mitigate the faint after-gate attack, as we discuss in the following section.

5.5 Mitigating the after-gate attack

Carriers with the short decays of approximately 300-400 ps that have been characterised could then be used to mitigate the faint after-gate attack. This is because Eve's attempt to mount such an attack using moderately high fluxes would result in delayed detection events that would alert the users to her presence. The sub-nanosecond separation between gates in GHz-clocked APDs is sufficiently narrow to allow delayed detection as a result of carriers with a decay on the order of several hundred picoseconds to be observed where they would be missed in slower, MHz-clocked systems [137, 195]. This hypothesis is illustrated in Fig. 5.6 and indeed we find that delayed detection can effectively reveal Eve's presence. However, we find that in this regime, traps at the multiplication region become the dominant contribution to delayed detection events, which we now examine.

We note that the measurement of overall detection probability needed for equation 5.1, rather than simply the APD count rate, is not straightforward. In general, it can be extracted simply by dividing the detector count rate by the laser repetition frequency. However, when we performed this using the same oscilloscope photon counting technique outlined in section 3.4, detection probabilities greater than unity were obtained. This is due to a ripple effect arising at large incident fluxes which means individual avalanches are counted more than once (also shown in Fig. 4.4 (b)).

Therefore, two further methods for determining the detection probability were developed. The first of these employed the oscilloscope in histogram mode. A histogram window of width equal to the inverse of the sampling rate of the oscilloscope (62.5 ps corresponding to a 16 GBit/s sampling rate) was placed over the section of

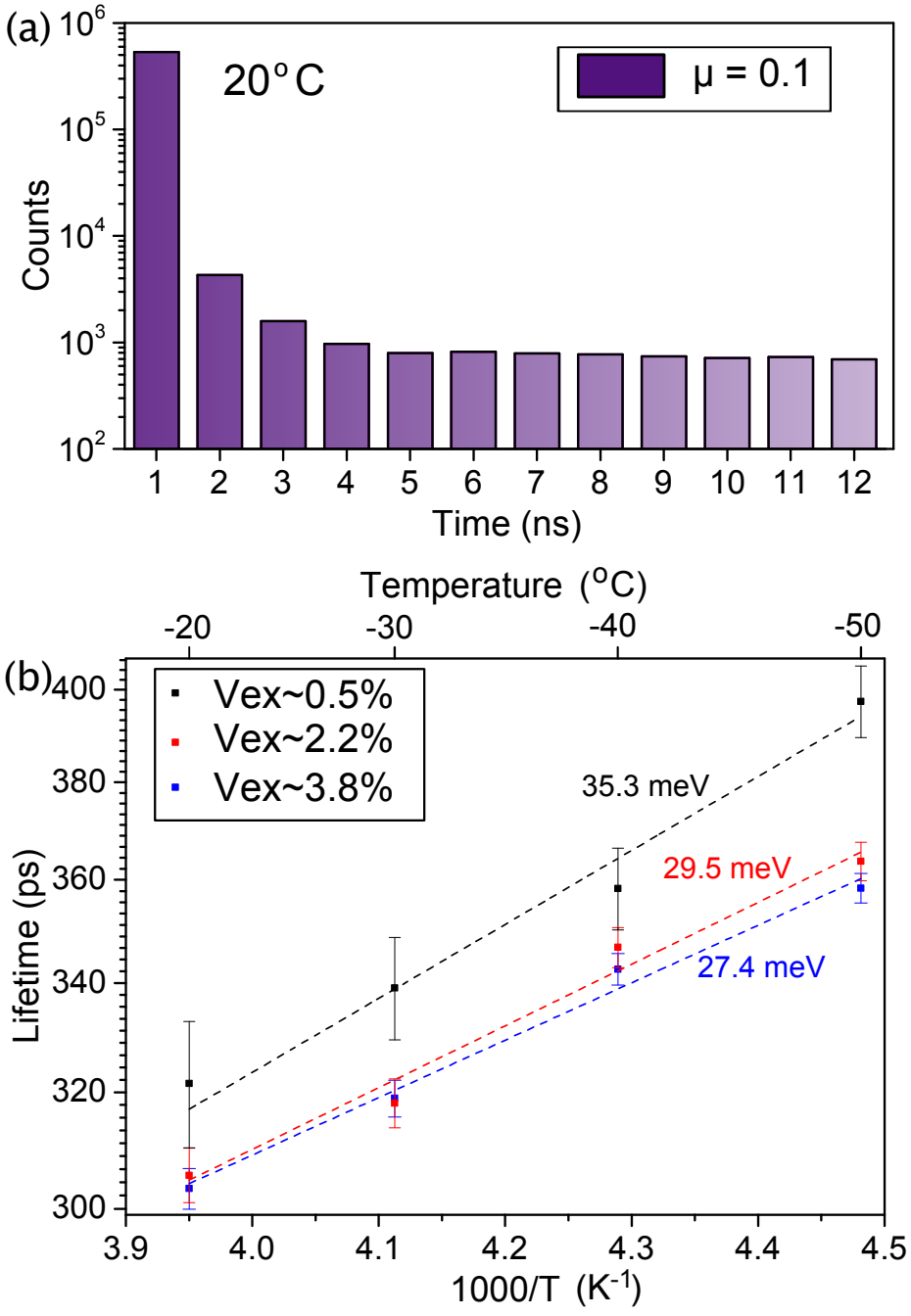


Fig. 5.5 **Characterising the material interface** *(a) Time-resolved histogram of detected counts of the APD under illumination of a pulsed laser with flux* $\mu = 0.1$*, clearly demonstrating an exponential decay in counts after the initial illuminated gate; (b) An Arrhenius plot showing the lifetime extracted from the histogram as a function of the inverse of the temperature, whereby the gradients allow for the extraction of the hole activation energy for each respective APD excess bias.*

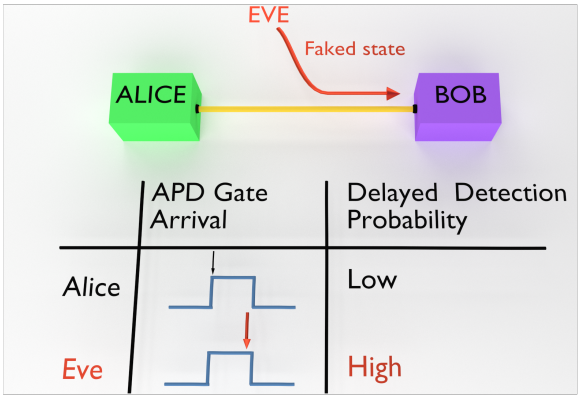


Fig. 5.6 **Delayed detection mitigating the after-gate attack** *Schematic demonstrating that when Eve mounts her after-gate attack by sending moderately strong pulses at the end of Bob's APD gate (compared to Alice sending single photons at the start of the gate), she has a high probability of inducing delayed detection in the subsequent gate and revealing herself.*

the APD waveform corresponding to the illuminated target gate. We analysed the histogram statistics and determined the proportion of hits that occurred above the discrimination level, thus giving a figure of the detection probability. This ensured only the target gate was measured and additional ripples were ignored, therefore the maximum achievable detection probability was unity. Unfortunately, limitations of the equipment mean this technique is inefficient at gathering a large statistical sample, therefore such a measurement needs to be run for an extended period to even out statistical fluctuations.

The second technique involved using a time-tagger with a configurable deadtime to analyse APD clicks. The deadtime eliminates the ripples and the resulting histogram was used to measure the detection probability in individual gates. This was suitable for regimes outside of the APD gate, where the detection probability is low, therefore the count rates are sufficiently low to avoid saturating the time-tagger. However inside the gate the count rates become too high for the instrument to register (the same problem reported in section 3.4). When used, a deadtime of 50 ns, corresponding to the laser period, was chosen.

We measured the detection probability at full (80 photons/pulse) and half (40 photons/pulse) power of an optical trigger pulse as a function of the arrival time of the laser pulse on the APD. We do this by varying the delay on the pulse generator providing the AC signal to the APD. Using these values as p_f and p_h respectively in Eq. 5.1 allows us to calculate the QBER resulting from Eve when considering the target gate and neglecting afterpulses and dark counts. The result is given for the APD

operated at two temperatures, 20°C and –30°C, as the black lines in Fig. 5.7 (a) and (c).

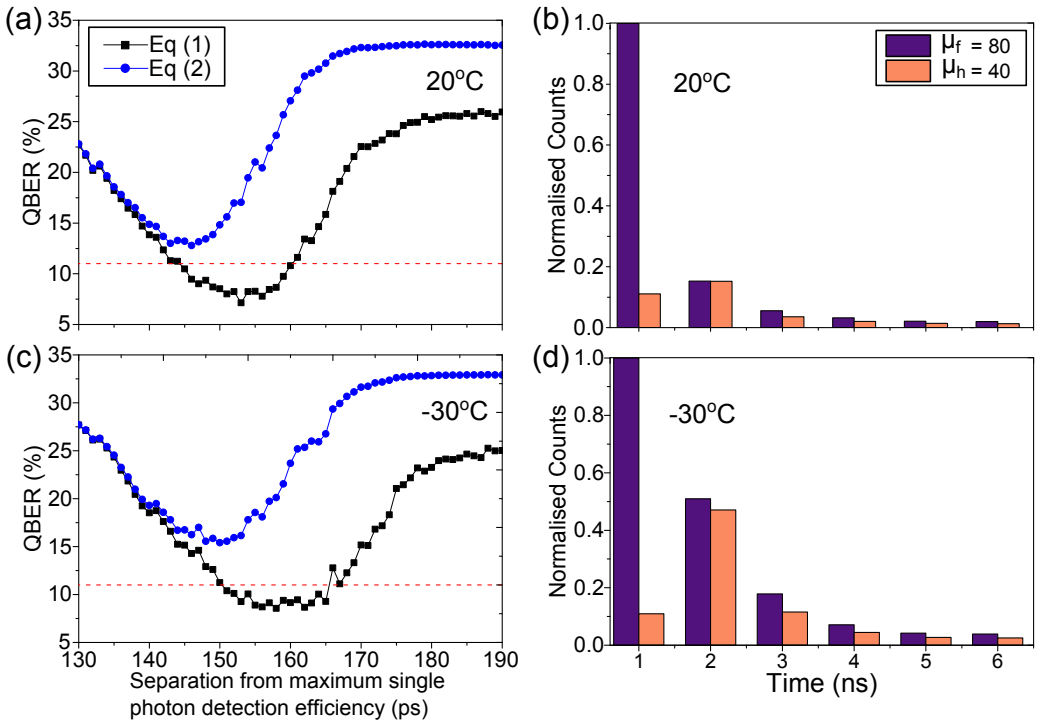


Fig. 5.7 **QBER introduced by the after-gate attack** *(a) QBER as a function of temporal separation from the maximum single photon efficiency delay value. The black line indicates the case where delayed detection is ignored and the QBER is calculated with Eq. 5.1 and Eve appears not to introduce a QBER greater than 11% and thereby remains undetected. When delayed detection is taken into account, as shown in the blue line calculated with Eq. 5.3, the QBER rises above 11% and she can be detected.; (b) Histograms taken at minimum QBER values showing detection probabilities in each time bin at 20°C. Under half-power illumination of* $\mu = 40$ *(in orange), bin 2 is always larger than bin 1, which would result in a QBER value of 50% in that bin.; (c) as (a) but measured with the APD at –30°C.; (d) as (b) but measured with the APD at –30°C.*

At a certain temporal separation from maximum detection, the QBER drops below 11% (illustrated as the red dashed line), reaching a minimum of approximately 7 % at around 153 ps at room temperature, suggesting Eve could mount such an attack at this delay and remain undetected. Either side of this trough, the QBER equals 25 % since either $p_f = p_h = 1$ around the centre of the gate or $p_f = p_h \approx 0$ outside of the gate.

To probe the effect of delayed detection, we examine the histograms in the vicinity of the superlinear regime, i.e. corresponding to the conditions of an after-gate attack, for two different temperatures, as shown in Fig. 5.7 (b) and (d). We note that for the cases where Eve is using the after-gate attack, a higher proportion of clicks actually

occur in the gate adjacent to the target gate (Gate 2 as opposed to Gate 1) when she chooses an incompatible basis to Bob, shown as the orange bars. Each delayed detection event has an equal probability of producing a correct or incorrect bit as they are uncorrelated with Alice's qubit preparation.

This underlines the importance of incorporating delayed detection events into the calculation of the QBER. To this end, we estimate the delayed detection probabilities under full and half power pulses and add them to the detection probability without delayed detection. This leads us to the following expression for the QBER:

$$Q' = \frac{2p'_h - (p'_h)^2}{2p'_f + 2[2p'_h - (p'_h)^2]}, \tag{5.3}$$

$$p'_{f,h} = p_{f,h} + \overline{p}_{dd}, \tag{5.4}$$

$$\overline{p}_{dd} = \frac{1}{4}p_{dd|f} + \frac{1}{2}p_{dd|h}. \tag{5.5}$$

The quantity Q' in Eq. (5.3) represents the QBER measured in the presence of the after-gate attack when delayed detection is taken into account. This is accounted for with the term $\overline{p}_{dd}$, which represents the average probability per gate of a 1-gate-delayed detection. The factor 1/4 (1/2) in the expression is due to having a click in Bob's detectors when his basis matches (does not match) Eve's basis in the previous gate. In Eq. (5.5), $p_{dd|f}$ ($p_{dd|h}$) is the probability of a delayed detection in gate n when a full-power (half-power) pulse impinged on the detector at gate $n-1$, represented as a violet-coloured (salmon-coloured) bar in Fig. 5.7 (b) (Fig. 5.7 (d)).

We further underline that this treatment approaches the QBER by incorporating all delayed detections, of which afterpulsing is a specific case, making this analysis more general. Earlier analyses have been solely concerned with afterpulsing, which is a delayed detection probability conditional on a legitimate click. This has resulted in the QBER previously being defined as follows (see section 1.5 and [198, 199])

$$Q = Q_{opt} + \frac{1}{2}P_a + Q_d + Q_b, \tag{5.6}$$

where Q_{opt} is the error which arises from imperfection in encoding apparatus, for example due to finite interferometer visibility or misalignment, P_a is the APD afterpulse probability, Q_d is the error arising from detector dark counts and Q_b accounts both for noise contributions from pulse broadening caused by fiber dispersion that could result in inter-symbol interference and Raman noise when quantum signals coexist with classical ones. As discussed earlier, the salmon coloured bars in the histograms of

Figs. 5.7 (b) and (d) at Gate 2 are greater than those in Gate 1. This would correspond to an afterpulsing probability, P_a, greater than 100%, therefore according to equation 5.6 the QBER would be 50%, confirming our original intuition.

We plot the resulting QBER from Eq. (5.3) with blue lines in Figs. 5.7 (a) and 5.7 (c). As is apparent from the figures, the 11% security threshold, typical of the BB84 protocol, is now overcome. This result highlights the effectiveness of the delayed detection at mitigating the faint after-gate attack.

By including contributions from delayed detection in Eq. 5.3, we assume Eve mounts her attack all the time. We therefore address the case whereby Eve only attacks a fraction of gates. In this case, the overall QBER would be smaller than the 11% tolerance and thus Alice and Bob would not abort their key exchange. However, Eve's information would also be smaller. Consequently, due to the key rate having a convex dependence on the QBER [10, 187], this case is still secure, as Alice and Bob's privacy amplification always overestimates Eve's knowledge of the key [34] (see section 4.7). Furthermore, this rationale overestimates Eve's chances to gain information because it assumes that the QBER is zero for the cases where Eve does not attack, whereas in the real case it clearly is larger than zero due to the delayed detection effect.

We also consider the case where Eve attempts to carry out a hybrid attack scheme, whereby she attempts to blind counts in Gate 2 and thus suppress any erroneous counts as a result of her after-gate attack on Gate 1. Whilst it has been shown that blinding attacks are ineffective against appropriately operated self-differencing APDs [184], this places the onus on the user and such devices are often improperly used. However, for Eve to blind Gate 2, due to the cancellation nature of the self-differencing circuit, she would also have to shine strong light on Gate 1, thereby negating her original attack.

5.5.1 Understanding the after-gate attack

For the demonstration of the attack presented in above in Fig. 5.7, we chose $\mu_f = 80$ and $\mu_h = 40$ as the full and half power fluxes respectively as these were values used in the original proposal in [137]. By expanding our measurement to examine a range of fluxes at room temperature, we were able to obtain a more general picture of the parameters that Eve could use (assuming delayed detections were neglected) but also to observe an overall trend, as shown in the measurement performed using a fast oscilloscope in Fig. 5.8.

The dark purple regions within the dotted line indicate a flux and delay combination which produces a QBER that is lower than 11 % when calculated using Eq. 5.1, within which Eve will choose to operate. The pale yellow parts in the top right of the

figure indicate a QBER of 25 % which occurs when $p_f = p_h = 1$. The dark speckles in the bottom section to the right of the purple band are where the count rates are comparatively low, meaning detection probabilities of zero are often measured. This overall trend of this figure implies that the closer to the centre of the gate Eve moves, the smaller the flux she should use to mount her attack. This suggests that this is an extension of the original proposed after-gate attack [137], whereby the APD is operating in linear mode and strong pulses of power P_{th} overcome the discrimination level and causes the detector to click, whereas pulses of power $P_{th}/2$ often do not and therefore rarely cause a click.

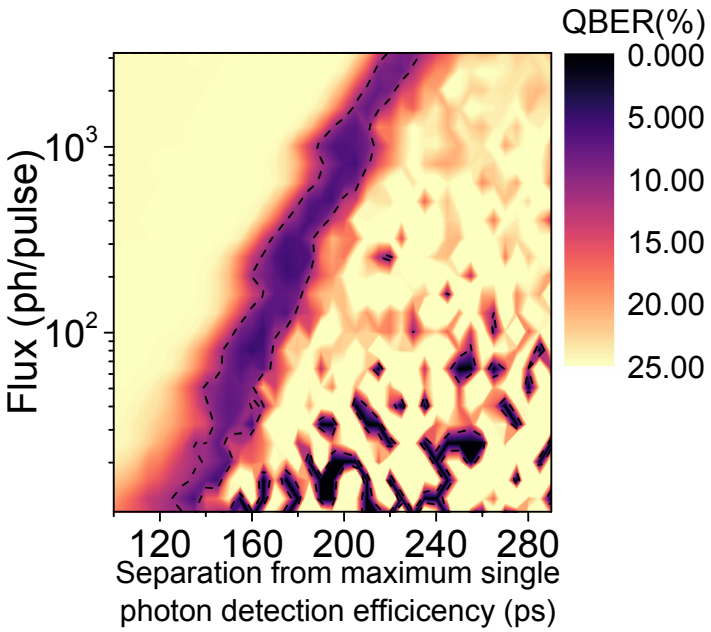


Fig. 5.8 **Eve's possible parameters** *A contour plot of the QBER as a function of the flux of the trigger pulse and APD gate delay with respect to the laser. The region inside the dotted line indicates where the QBER is lower than 11 % and thus Eve can mount a successful attack in this parameter space if delayed detections are neglected.*

5.5.2 Delayed detection events for mitigating the after-gate attack

As mentioned earlier, the origin of delayed detection when the APD is subjected to the after-gate attack is predominantly due to carrier trapping in the multiplication region. At room temperature, the lifetimes extracted from Fig. 5.7 (b) are comparable to the case shown in Fig. 5.5 (b). However, at –30°C, the lifetimes become much longer than those shown in Fig. 5.5 (b) for the same temperature, by approximately 2-3 times. This suggests the existence of deeper traps and that these traps, rather than the material

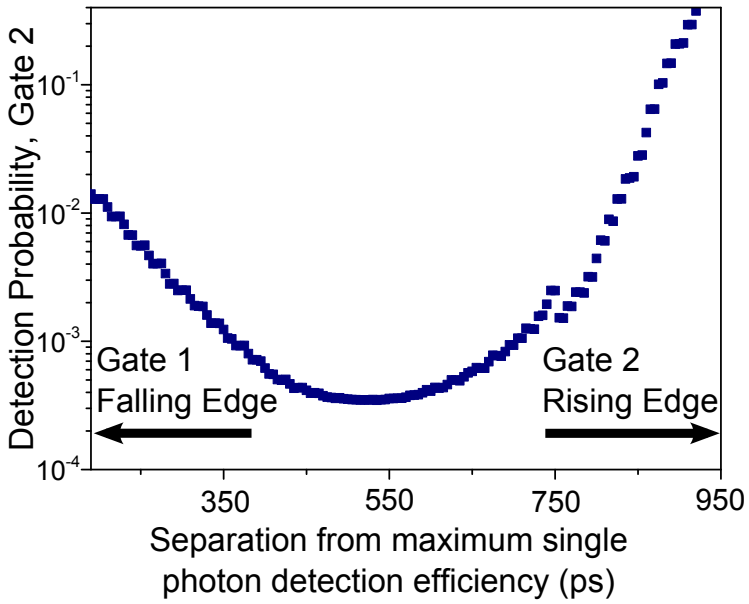


Fig. 5.9 **Origin of delayed detection** *Detection probability in Gate 2 as a function of temporal separation from maximum single photon detection efficiency for APD 2. The peak in the left-hand side of the figure can be explained by the dominance of trapping in the multiplication region.*

interface, are responsible for the delayed detection in the after-gate attack. We believe these deeper traps are located in the multiplication region.

This is supported by measuring the detection probability in the adjacent gate (Gate 2 in Fig. 5.2) as a function of separation from the maximum detection for APD 2, as shown in Fig. 5.9. Reading left to right, the laser is moving away from the end of Gate 1 and approaching the start of Gate 2. The detection probability initially decreases as the laser approaches Gate 2. Here, impact ionisation is occurring and therefore carriers are multiplied and a portion of these multiplied carriers are trapped in the multiplication region, shown in purple. The high detection probability on the left-hand side roughly coincides with the QBER dip, underlining that delayed detection largely arises from trapping in the multiplication layer. If the interface were the major contributor, the detection would continue to increase the closer to Gate 2 the laser is as the carriers have a progressively shorter time to decay before Gate 2 is activated. However, at a certain point the probability flattens and then begins to increase, an observation which is consistent with interface trapping, suggesting it starts to take over once carriers cease to become trapped in deep levels at the multiplication region.

5.6 Best practice for choosing an APD gating frequency

Using the discovery of delayed detection allows us to define the best practice for choosing a suitable gating frequency for QKD. For our analysis at two individual temperatures, 20°C and –50°C, we only consider trapping at the material interface. This is the more conservative definition from a security point of view, as it requires higher gating frequencies to maintain the delayed detection required for preserving the protection against the after-gate attack. This range of gating frequencies fulfils two criteria; (i) the gating frequency is low enough to separate adjacent gates temporally such that a click in the first has a small enough probability to have a delayed detection in the second without raising the QBER above the tolerance threshold of 11% under operation in the absence of Eve, assuming Alice sends a flux of $\mu = 0.4$ photons per pulse; (ii) equally, the gating frequency is high enough such that Eve would cause clicks in the gate adjacent to her target gate with a large enough probability to raise the QBER above the aforementioned threshold, which we examine for a conservative attacking flux of $\mu = 20$ photons per pulse that is favourable for hiding Eve's presence (see section 5.5.1). Our simulation result is shown in Fig. 5.10, with the narrow white band indicating a regime where the APD is neither too 'Noisy' nor 'Vulnerable'. Due to the longer carrier decays at lower temperatures, we note that lower temperatures are more favourable for slower gating whereas higher temperatures are more suited to faster gating. Most significantly, gating frequencies of around 1 GHz, which are commonly used for QKD experiments (e.g. [13, 200, 63]) as well as in this study, fall in the white region, suggesting these to be optimal values for QKD.

5.7 Conclusion

In conclusion, we have investigated two sources of trapping of carriers in InGaAs APDs: at the potential well arising at the interface between the APD absorption and charge regions, and at deep traps in the multiplication region. In characterising the carrier lifetime at the heterojunction, we have provided the first explanation for short decays observed in fast-gated APDs. We have determined that in the after-gate regime, however, the major contribution to delayed detection events that can provide enhanced security arise from traps in the multiplication region. We have provided the first evidence that fast-gated APDs can be used to mitigate the after-gate attack due to the additional contribution to the QBER that arises from delayed detection events. By exploiting the intrinsic imperfection of the material interface, we were able to bound the appropriate APD gating frequency suitable for use in QKD. The faked state

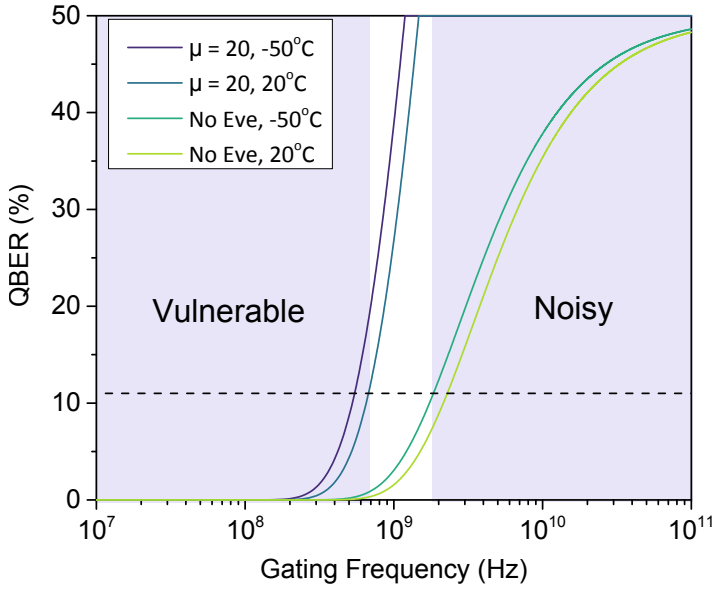


Fig. 5.10 **Useable gating frequencies** *Quantum bit error rate (QBER) as a function of gating frequency at 20°C and –50°C. The central white region indicates suitable operation, where the APD is both safe from the after-gate attack (with an attacking flux of $\mu = 20$ photons per pulse) and has sufficiently low noise to make QKD possible (with an average flux of $\mu = 0.4$ photons per pulse).*

attacks covered in this and the preceding two chapters all present the legitimate users opportunities for detecting Eve as they require her to actively interact with the QKD setup. Therefore, it is more favourable for her to act as passively as possible so as to operate undetected. The following chapter explores an imperfection in APDs which could allow her to do so.

Chapter 6

Backflashes

6.1 Introduction

The previous chapters in this thesis have addressed ways in which Eve actively interacts with Bob's apparatus in order to learn the secure key. This presents more of an opportunity for her presence to be detected than when she behaves passively. Avalanche photodiodes can emit light under certain conditions, which presents a backdoor that Eve could exploit to learn secure bits by simply measuring this emitted light, known as backflashes. In this chapter, we characterised the quantity of backflashed light for a GHz-gated self-differencing single-photon avalanche photodiode (SD APD) and related it to the information leakage to Eve. By quantifying the effect of backflashes on the secure key rate, we have determined that the security implications of this phenomenon are negligible.

6.2 Light emission from avalanche photodiodes

The phenomenon of p-n junctions emitting light when reverse biased to breakdown was first observed for silicon devices in [201]. However, it wasn't until 2001 when this concept was first thought of as a security problem for QKD [202]. As this was still concerned with silicon devices, which are unsuitable for wide-spread fibre optics QKD implementations, studies on InGaAs APDs are of most interest and will be the focus of this chapter.

Only the past few years have yielded research into more commonly used InGaAs APDs for QKD. The most significant study was performed in [203] on 2 types of detector, one commercial and one developed by the group, both of which were gated at relatively low frequencies of 50 kHz. The authors defined a metric, known as

information leakage, for measuring how detrimental the level of backflashes for a particular device could be for a QKD system. It is given as follows

$$P_L = \frac{N_B}{N_A \eta_{det} \eta_{ch}} \tag{6.1}$$

where N_B is the number of detected backflashes, N_A is the number of detected valid APD counts (i.e neglecting dark counts), η_{det} is the detection efficiency of the monitoring detector, and η_{ch} is the channel loss between the APD under test and the monitoring detector. The authors found values of information leakage for their detectors to be 9.8% and 6%. This means that for their least vulnerable detector, for approximately every 16 raw bits that Bob obtains, Eve will obtain 1 bit.

Such a significant proportion suggests this security loophole could be quite dangerous and as such a countermeasure could be necessary, whether that is a software modification (such as additional privacy amplification) or hardware one (additional components). A natural idea, as suggested by the authors, would be the placement of an isolator at Bob, echoing a countermeasure against Trojan horse attacks [34]. Whilst this would undoubtedly be effective, the introduction of additional components at Bob is to be avoided due to the extra loss they would incur, thus providing a penalty to the secure key rate. Therefore it is more desirable to reduce the inherent backflash phenomenon at the APD. In order to understand how this may be possible, it is useful to first explore the origin of backflashes.

It has been suggested in the literature that backflashes can arise from two effects. The first of these is recombination [204]. Once a photon is absorbed in the InGaAs region, an electron-hole pair is generated. The hole is swept towards the InP multiplication region and there many more carriers are generated through impact ionisation. In this process a number of holes accumulate in the valence band and the same number of electrons are present in the conduction band which can then recombine and generate a photon. As this occurs in the InP region, where the band gap is 1.35 eV at room temperature [205], the emitted light would peak at a wavelength of around 920 nm.

The second possible origin is a relaxation of the large number of hot carriers that are generated in the multiplication region [203]. As the carriers that arise from impact ionisation have a range of energies, light emitted this way would be expected to be broadband and would include the telecom wavelengths.

Several studies have examined the spectral characteristics of backflashes [203, 206, 207], although they have not been able to conclude which phenomenon contributes to the origin of backflashes. This is largely due to the use of a second InGaAs APD as a

monitoring detector. This has meant that backflash detection has been restricted to the spectrum to which these APDs are sensitive. ~~namely the telecom band at around 1550 nm.~~ Furthermore, all aforementioned the studies have not corrected for the APDs' spectral dependent efficiency, hence the trends have tended to correlate with the APDs' quantum efficiency.

One study appears to have analysed a wide spectral range and corrected for the spectral sensitivity of their system [208]. They observed a large peak at around 900 nm, correlating with recombination, and then a much fainter broad distribution, suggesting the hot-carrier relaxation. However, no details of their system are given, making it difficult to make a conclusive judgement.

In both hypotheses, the rate of backflash emission is related to the number of carriers generated in the multiplication region. As such, under normal operation, it would be desirable to limit the charge in the APD as much as possible without severe detriment to device performance. For gated APDs, this can simply be done by applying narrow 'ON' gates to the device such that the time over which the avalanche grows is limited [203]. This naturally suggests that faster-gated devices would provide an inherent reduction in the charge and hence emit fewer backflashes. This is a particularly attractive solution as the key rate would not be adversely affected through the need for either further privacy amplification or components with additional loss. Indeed, operating detectors with higher clock rates would, in fact, improve the secure key rate.

In this study, we study the information leakage of GHz-gated InGaAs APDs and find it to be an order of magnitude lower than the previous best performance in the literature. Using this finding, we derive a new bound for the secure key rate that incorporates backflashes. We also measure the backflash dependence on the APD current and thereby confirm their origin to be the InP multiplication region.

6.3 Experimental setup

An InGaAs/InP APD is chosen as the device under test. It is thermoelectrically cooled to –30°C where the breakdown voltage is 62.16 V. When driven with a constant DC bias of 59.66 V and a peak-to-peak 1 GHz AC signal of 10 V, the APD exhibits a detection efficiency of 17%, a dark count probability of 1.9×10^{-6} and an afterpulse probability of 5%.

For investigating the information leakage of a GHz-gated APD, a separate monitoring detector with sufficiently low dead time (i.e. on the order of nanoseconds) and high detection efficiency is required to gain an accurate picture of backflashes. The deadtime of the monitoring detector has proved to be a limiting factor in previous

studies, meaning investigations have been restricted to using free-running APDs to monitor slower-gated detectors [203]. By using superconducting nanowire detectors (SSPDs) which have detection efficiencies exceeding 80% and deadtimes of only several nanoseconds (as well as emitting no backflashes themselves), it is possible to conduct the first experiment into backflashes of fast-gated detectors. The APD is illuminated with a C-band pulsed laser diode with a repetition frequency of $1/64$ of the APD gating frequency (15.625 MHz). The flux is controlled using a variable optical attenuator. We illuminate the APD with 0.1 photons/pulse, a flux typical for QKD, at the start of the APD gate. By extracting the counts from the illuminated bin of the APD detection histogram (see Fig. 5.5(a)), we can obtain a value for use in Eq. 6.1. The backflashes are then quantified by measuring the count rate of a superconducting nanowire single-photon detector (SSPD) used as a monitoring detector, N_B, multiplied by its detection efficiency, η_{det}, which is 80% and the channel loss, η_{ch}, which is 0.78. The light enters port 1 of a circulator and port 2 is connected to the APD. Emitted backflashes then re-enter the circular and exit via port 3, after which they are measured with the SSPD. The detected APD counts and backflashes are interpreted with a time-tagging single-photon counter. This is illustrated in Fig. 6.1.

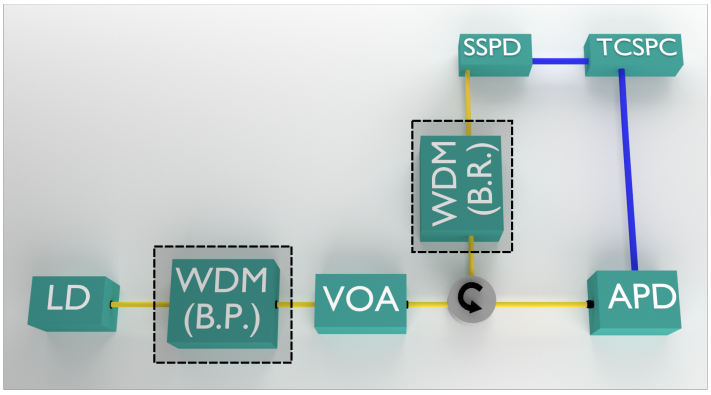


Fig. 6.1 **Experimental setup** *Schematic of the experiment used to investigate APD backflashes, with the dotted line surrounding the WDMs indicating they were only used in one experiment. The WDMs were either used as band pass or band reject filters. LD: laser diode; WDM (B.P.): wavelength division multiplexer (band pass); WDM (B.R.): wavelength division multiplexer (band reject); VOA: variable optical attenuator; SSPD: superconducting single photon detector; TCSPC: time-correlated single-photon counter*

6.4 Extracting the backflash rate

In an ideal case, any light detected by the SSPDs can be attributed to backflashes. However, backreflections from the APD are also detected and can artificially raise the SSPD count rate. An example of this is shown in the histogram of SSPD detection events with the APD DC and AC disabled in red in the top graph of Fig. 6.2. The peak features at approximately 17 and 49 ns can be attributed to backreflections and they dominate the SSPD detection events when the APD is on, as shown in the blue bars of the same figure. It is also interesting to note that the blue bars corresponding to backflashes are reasonably uniformly distributed across the histogram, with the exception of the second backreflected peak. At this point of approximately 49 ns, the blue bars have a much larger amplitude (around 100 counts rather than 40) which suggests that this peak corresponds to reflection from the APD surface itself and that the backflashes are strongly correlated with APD detection events. This is to be expected as when the APD is illuminated, there is a high probability of carriers being generated in the multiplication region after photo-absorption.

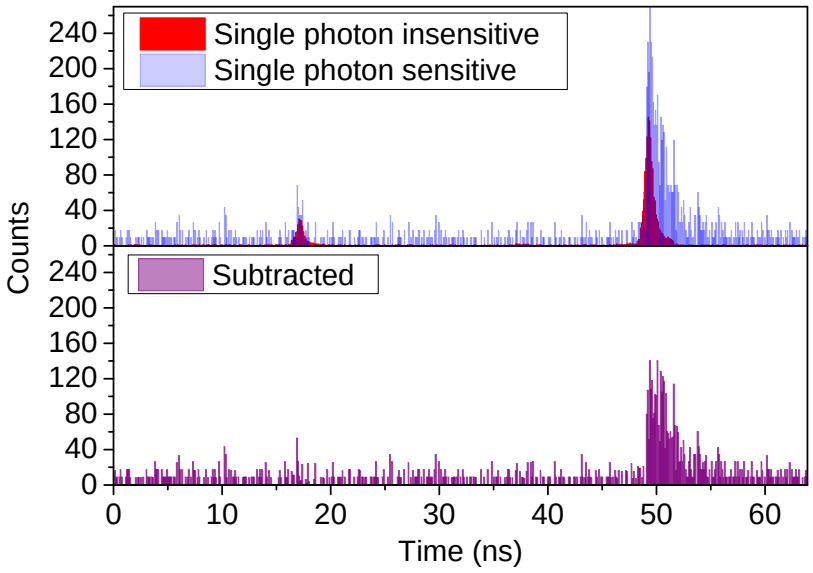


Fig. 6.2 **SSPD histogram** *Top: Histogram of the detection events on the SSPD when the APD is illuminated with a flux of* $\mu = 0.1 photons/pulse$*. The red bars show the histogram when the APD is off and only SSPD dark counts and backreflections are detected. The blue bars are with the APD on and a large DC of 61.66 V applied. Bottom: Subtracted histogram with backreflections removed, leaving only backflashes*

In order to obtain a true measure of the information leakage, it was necessary to isolate the backreflections. A simple technique for this is simply to neglect them in post processing. This was done by subtracting the SSPD histogram with the APD

turned off, so that only backflashes were measured, shown in the bottom graph of Fig. 6.2. This large peak also at around 49 ns supports the hypothesis given above that the backflashes are correlated with APD detection events.

A second technique was also used by means of spectrally filtering the backreflected light. A wavelength division multiplexer (WDM) centred at 1550.12 nm was placed in the transmission path and used as a band pass filter. 3 additional WDMs were then used between the circulator and SSPD and as a band-reject filters. This combination was used to ensure all backreflected light was rejected. The spectra of the unfiltered laser, the laser with the band-pass WDM and the laser with both WDMs is given in Fig. 6.3 and shows a rejection of at least approximately 20 dB between the highest points of the filtered and raw signals respectively. We expect the rejection to be better than this as we are filtering for photons reflected from the APD surface rather than directly transmitted and this should therefore easily remove any contributions from backreflections.

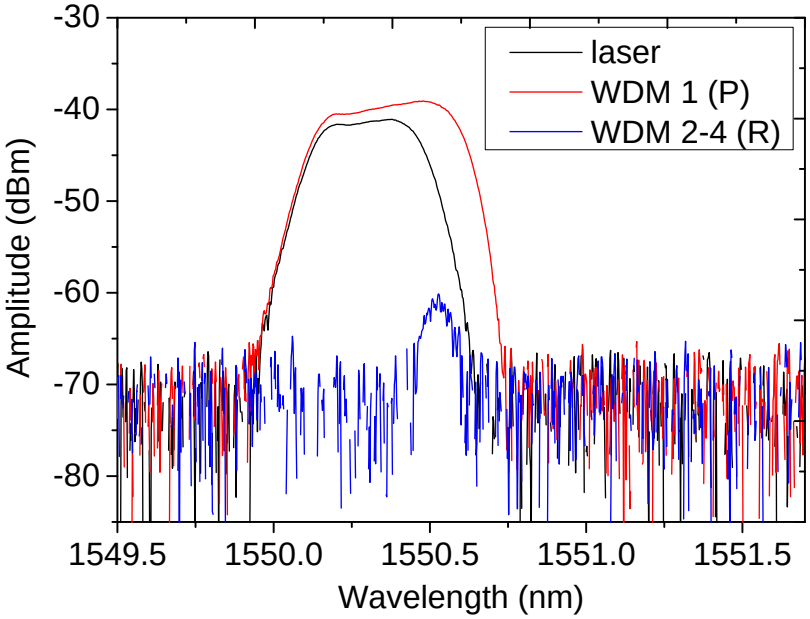


Fig. 6.3 **Wavelengh division multiplexer (WDM) characterisation** *Laser spectrum measured with an optical spectral analyser (OSA) separately, with a band-pass WDM and band-pass followed by 3 band-reject WDMs.*

6.5 Information leakage

The SSPD count rate was measured simultaneously alongside the APD detection efficiency using the two aformentioned techniques as well as the uncorrected histograms

to provide an absolute upper bound on Eve's information. The information leakage was then extracted in each case using Eq. 6.1 and is plotted in Fig. 6.4. The previous state-of-the-art from [203] was also plotted with a purple star as a comparison.

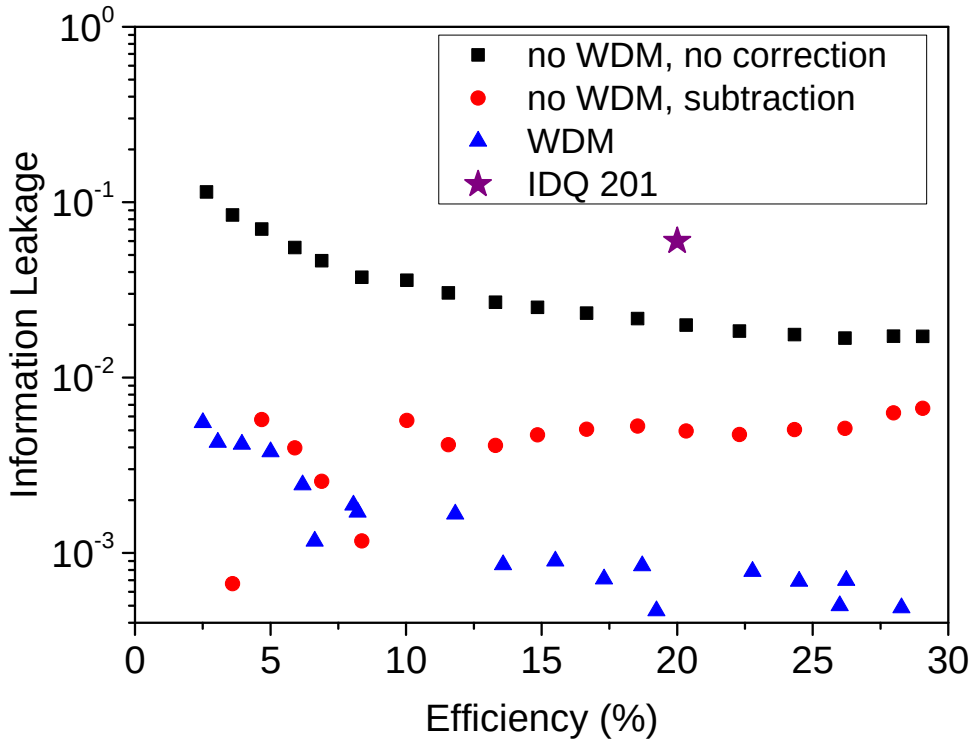


Fig. 6.4 **Information leakage** *plotted as a function of the APD single-photon detection efficiency with the three aforementioned measurement techniques. The black squares show the information leakage calculated using the raw SSPD count rate, the red circles with the subtraction of the histogram with the APD turned off and the blue triangles using the wavelength division multiplexers (WDMs). The purple star indicates the corresponding information leakage for a commercially available APD, IDQ 201. The fact that the data taken with the WDM does not overlap with that taken without supports the hypothesis that backflashes are also filtered out by the WDMs. Indeed, the increasing discrepancy arises from the SSPD count rate in the presence of the WDMs remaining approximately constant at the dark count level.*

We see where no WDM is used and the backreflected counts are subtracted afterwards, the data appears initially very noisy at low efficiency. This is due to the SSPD count rate being similar to its dark count rate, which suggests the rate of backflashes is very low. The data then appears much smoother from an efficiency of 10% as the rate of backflashes increases. As the information leakage remains more or less constant from then on, this suggests the relationship between backflashes and APD counts is linear. By comparing this to the IDQ 201 detector at the same detection efficiency of

20%, we see an order of magnitude improvement in the information leakage, which supports the hypothesis that shorter gates will emit fewer backflashes.

For the case in the presence of the WDM, the information leakage is lowest. This is due to the fact that the SSPD count rate is very low, comparable to its dark count rate, suggesting the WDM is also filtering a large proportion of backflashes. This is reinforced by the relative noisiness of the data arising from the spontaneous nature of dark counts. Furthermore, the information leakage decreases with increasing efficiency, because the SSPD count rate is remaining around its dark count level whilst the APD counts are increasing. This explains why the red and blue points do not overlap, as they would be expected to if only backreflections were neglected.

Using the value for information leakage, which is a direct measurement of Eve's information, we can derive a new secure key rate in the presence of backflashes. This has been partially investigated in [138] where the authors approach the derivation of the key rate from a photon number splitting perspective and treat the information leakage as 'tagged' bits, but originating from Bob rather than Alice [209, 210]. However, the authors in [138] assume the backflash probability, and therefore information leakage, remains constant over all distances, which means they obtain a very pessimistic estimate for the secure key rate. In reality, as the information leakage is dependent on an APD click, the APD click probability should also be incorporated into this analysis so that the key rate is affected by the same proportion, regardless of distance. We use a modified version of the key rate for single-photon BB84 given in [138] and from Eq. 1.3 as follows

$$R \geq qP_{click}\left[(1-P_L)\left\{1-h(e)\right\}-\left\{fh(e)\right\}\right] \tag{6.2}$$

where q is the basis choice probability, P_{click} is the probability of a click on a detector, P_L is the information leakage (defined in Eq. 6.1), $h(x)$ is the binary Shannon entropy and f is the error correction efficiency. For more detailed definitions, I refer the reader to section 1.5. It is interesting to note that by simply multiplying the information leakage term by the click probability in the key rate definition from [138], thereby including a dependence of the backflash probability on the APD detection probability, that equation reduces to Eq. 6.2.

Using detector characteristics from this study we plot the key rate as a function of distance for several values of information leakage, namely zero (the solid black line), 6×10^{-2} (blue points), which was the previous state-of-the-art and 5×10^{-3} (red points), as measured in our own setup, as shown in Fig. 6.5.

As an information leakage of 0.5% has a negligible effect on the key rate, an isolator would not be needed as a countermeasure since even with a very low insertion

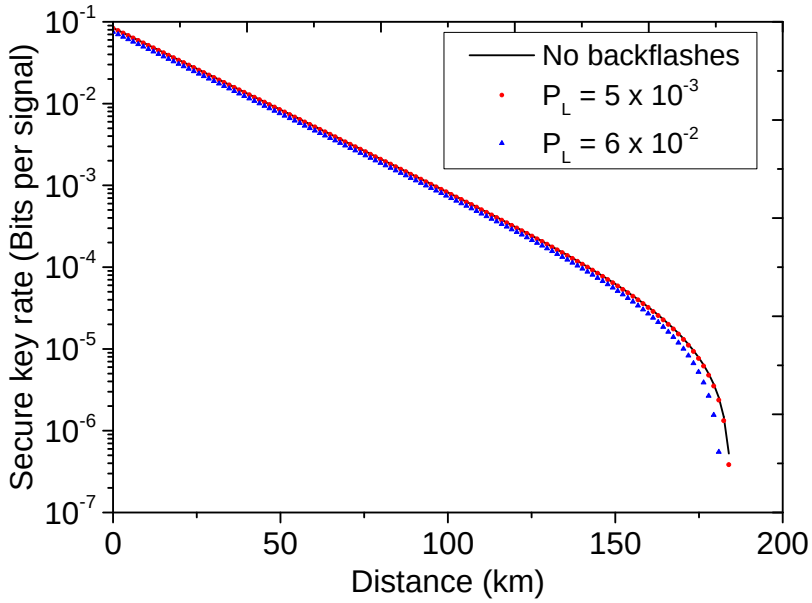


Fig. 6.5 **Secure key rate in the presence of backflashes.** *Secure key rate plotted in the absence of backflashes, with the measured information leakage and previous state-of-the-art. Even with $P_L = 6\%$, the effect on the key rate is negligible, as the term P_L gives the exact amount by which the key rate is reduced.*

loss of 0.2 dB, it would have a greater impact on the key rate. This result provides strong evidence that backflashes are not a significant threat to QKD, even for slower gated detectors where the information leakage is potentially larger.

6.6 Origin of backflashes

As a second experiment to probe the origin of the APD backflashes, we switch off the laser and remove the WDMs in Fig. 6.1 and measure the backflashes with the APD kept under dark conditions. We measure the SSPD count rate as a function of the APD dark current by adjusting the DC bias to the APD. The result is given in Fig. 6.6.

Initially the SSPD count rate remains at the dark count level until the APD current reaches a value of approximately 10 nA. After about 100 nA, the data appears to follow a linear trend and this is confirmed by fitting the data points. This finding supports the hypothesis that backflashes arise from carriers in the multiplication region; a higher dark current arises from the larger electric field increasing the avalanche probability, thereby generating more carriers which cause backflashes.

To confirm the avalanche charge is the dominant factor in backflash emission, we keep the APD in dark conditions and perform the same measurement, this time with the AC signal to the APD switched off. This is shown in Fig. 6.7. The data points

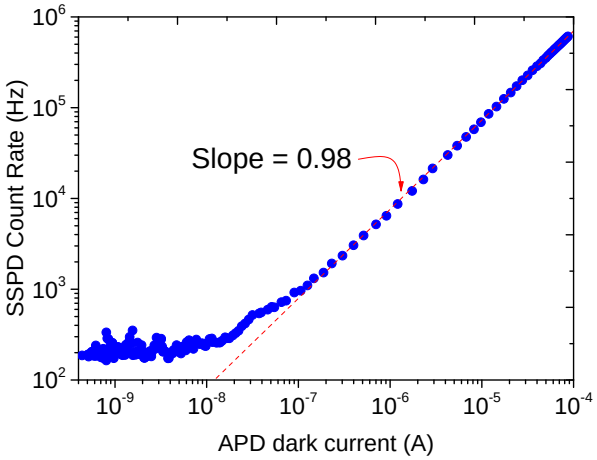


Fig. 6.6 **SSPD count rate as a function of APD dark current.** *The linear relationship between the two strongly points to backflashes originating in the InP multiplication region.*

overlap almost completely, which suggests the exact biasing technique is not important in determining backflash emission, rather the avalanche charge, and hence the number of carriers, is the numeric of interest.

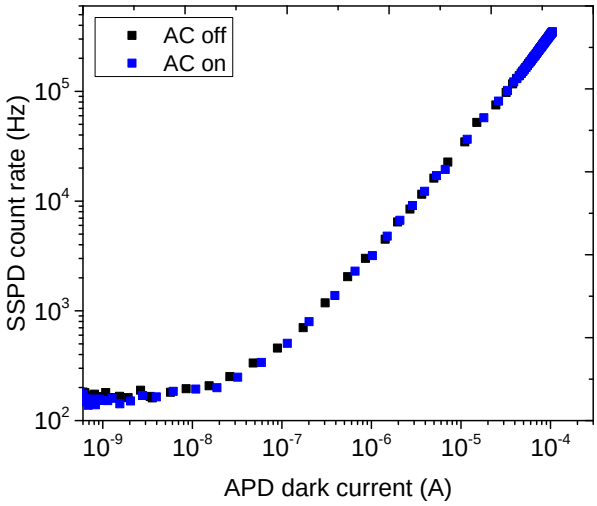


Fig. 6.7 **SSPD count rate as a function of APD dark current in the presence and absence of the APD AC gating signal.** *The linear relationship is still preserved with the AC off (shown in black squares) and the data closely matched that taken with the AC on (blue squares), highlighting that the avalanche charge is the parameter of interest.*

6.7 Conclusion

In conclusion, we have performed the first investigation of backflashes in GHz-gated APDs. As suggested in the literature, we have found that shorter APD gates reduce the backflash rate and therefore Eve's information due to the reduction of the avalanche charge within the device. A new definition for the secure key rate in the presence of backflashes was developed and it was shown that backflashes in both fast- and slow-gated APDs have a negligible effect. Preliminary measurements to probe the origin of backflashes were carried out and it was confirmed these arise in the device multiplication region. Further measurements, namely by analysing the spectral characteristics of this emission, will be required to conclusively state whether they arise from recombination of electron-hole pairs or relaxation of hot carriers.

Chapter 7

Conclusions and Outlook

7.1 Novel contributions

- Best practice criteria for the operation of self-differencing avalanche photodiodes has been outlined for the first time. This highlights the importance of operating devices appropriately, particularly with the choice of discrimination level, as failing to follow such guidelines results in security loopholes that an eavesdropper could exploit. This paves the way for standards to be developed, easing the widespread implementation of quantum key distribution.

- A secure measure against the blinding attack was proposed and demonstrated using an intensity modulator. This proof-of-principle was done using a lithium niobate ($LiNbO_3$) device to introduce extinction between adjacent APD gates and thus prevent avalanche cancellation. It was found that only a 0.06 dB extinction was required to completely eliminate the blinding attack. It was also demonstrated that existing phase-encoded QKD protocols already possess inherent protection against continuous wave blinding.

- Delayed detection events were discovered to be an effective measure for mitigating the after-gate attack on APDs. The origin of these delayed detections was probed, with contributions arising from deep traps in the APD multiplication region and material interface contributing. These detection events were incorporated in a new calculation of the QBER, showing that Eve cannot mount her attack and remain undetected. Bounds on useable APD gating frequencies were also established.

- The first investigation of backflashes in GHz-gated APDs was carried out. An information leakage of 5×10^{-3} was measured for these devices, an order of

magnitude less than that for slower gated devices shown in the literature. This confirms the result that shorter gates exhibit fewer backflashes. The effect of backflashes on the secure key rate was established and it was shown that the security risk is minimal.

7.2 Future Work

7.2.1 Implementation security

The security of self-differencing avalanche photodiodes (SD APDs) has been investigated in this thesis and it has been found that these devices contain an inherent level of protection against attacks. By explicitly defining the best practice for operating these devices, blinding attacks were mitigated. It would therefore be useful to extend this approach of 'best practice' to other classes of detectors, particularly gated APDs without self-differencing circuitry and superconducting nanowire single-photon detectors (SSPDs) as these are widely used in the quantum key distribution (QKD) community. Indeed a number of the best practice criteria are applicable to fast-gated detectors in general, such as the appropriate setting of the discrimination level. Other components in the system would of course need standards defined as well. For example, the proportion above threshold that Alice should bias her laser diode in order to reduce the fluctuation in her output photon flux would need to be stringently defined. In a system that uses multiple lasers, which is common for free-space implementations (such as [58]), the indistinguishability would need to be bounded between the sources such that Eve cannot gain information from other degrees of freedom. Indeed, this has been partly investigated using the Hong-Ou-Mandel effect [211], but even small deviations produced a significant reduction in the obtained secure key rates, suggesting more work is needed. This would facilitate the definition of standards, which is ongoing in the work being carried out by ETSI, allowing QKD systems to be officially certified and enter everyday life. To do this, security requirements or assumptions for each component need to be defined. The parameters need to be identified, measured and their deviation from the requirements quantified. After this, the information leakage can be estimated to bound the Eve's information. Finally, countermeasures can be introduced, whether in software (such as additional privacy amplification) or hardware (such as the intensity modulator, IM, in the APD blinding case).

To focus on the receiver, a number of requirements need to be fulfilled. Each detector must have the same response to the same encoded state, independent of any secondary degrees of freedom which are encoded on the optical pulse. Furthermore, the detection efficiency must also be independent of these secondary degrees of freedom. For example, in a phase-encoded scheme, Eve must not be able to alter the polarisation of Alice's qubits in order to bias Bob's detections. This is particularly relevant to SSPDs, which are polarisation sensitive [212], but still needs to be explicitly established for APDs. All the detectors must be statistically identical and the probability of detection by each device must be independent of the measurement

settings. In essence, the detectors should, as closely as possible, behave according to the security model, which consists of a beamsplitter, with a transmission arm equal to the device's detection efficiency, followed by a detector with a detection efficiency of 100%.

Intensity modulation was found to be an effective way to mitigate blinding in the case of inappropriate operation. However, the IM used in the study contains a significant insertion loss of at least 2.5 dB since it is designed for high extinction operation. This loss penalty could significantly limit the achievable distance. Since only low extinction is required (0.06 dB), it would be useful to demonstrate the effectiveness of an IM with a shorter waveguide and subsequently smaller insertion loss. Although the IM was shown to be effective and a short discussion surrounding security was presented, a complete security proof incorporating this is still lacking. By including blinding and IM as a countermeasure, much as photon-number-splitting and decoy states are included, this attack can finally be discounted and the security of APDs against it assured. Furthermore, demonstrating this countermeasure in a complete QKD system, also employing modulation driven by a true QRNG would provide further assurance that it is effective in preventing blinding attacks. Finally, the IM, as with other components in the QKD system, would need standards to certify its operation.

Delayed detection events were demonstrated to be effective at mitigating the after-gate attack. However, this effect relies on imperfections within APDs to provide such protection. If better devices are manufactured in the future (with a better InGaAsP grading layer or an InP multiplication layer with fewer traps), this protection could disappear. Therefore, analysis of the trade-off between this protection and the potentially more efficient devices would need to be performed. Ideally, APDs would be tailor-made for QKD applications and would include this consideration in their manufacture. Alternatively, a suitable countermeasure could be proposed and demonstrated: photon-number resolving InGaAs APDs, currently under development [113], could be used which would be able to detect abnormal photon-fluxes; or more precise electronics which could distinguish clicks outside of the normal detection window within an APD gate [62].

A further open-question for detector attacks is that of detection efficiency mismatch [143, 144]. This arises from the individual detectors at Bob being distinguishable, specifically with regards to their detection efficiency as a function of photon arrival time. Eve can exploit this by choosing the arrival time of her faked state pulses to coincide with the higher detection efficiency of the detector she would like to control. Furthermore, this discrepancy can be further exacerbated if she interferes with

the calibration routine before QKD is performed [145]. However, if Bob is able to randomise his detectors to detect bit '0' or bit '1', known as detector symmetrisation, then this attack can be subverted as the average detection responses would be the same across all bits and bases. Whilst this has been demonstrated in free-space polarisation encoding QKD [213], it is yet to be shown in fibre-based phase encoding schemes which are the current state-of-the-art. Most likely, this would involve the use of phase modulators that induce additional shifts of π and $\frac{3}{2}\pi$.

7.2.2 Quantum key distribution

In a more general sense for QKD, reducing the size of QKD systems is an ongoing goal and photonic integrated circuits have been subject to intense research. Whilst receiver chips that contain decoding apparatus that are usually done with bulk components have been demonstrated [15, 214, 215], the integration of APDs has not yet been achieved. Receiver chips could also then include specifically fabricated intensity modulators with low extinction to add security against blinding attacks as a characteristic of this integration.

Achieving larger secure key rates is an ongoing challenge for QKD. One of the most apparent ways to do this is to simply increase the clock rate of the QKD system. However, APDs are limited in this respect due to the necessity to have sufficiently long gates to allow the avalanche to grow to overcome the discrimination level. Analysing this trade-off would ensure APDs are operated to their optimum capacity. A further bottleneck exists in the electronics within the QKD systems themselves such that they cannot process the large volumes of data that occur at short distances, thereby limiting the secure key rates at low loss [13].

Whilst QKD is a promising answer to the threat to cryptography posed by quantum computers, other avenues have also been explored. These fall under the umbrella term of post-quantum cryptography and are based on mathematical problems for which no quantum computing algorithm yet exists. For the most part, post-quantum cryptography and QKD have developed and operated separately, but a security system combining the two approaches would add an extra layer of assurance (in case one aspect is compromised) and could increase the secure bit rate offered by QKD alone [60].

7.2.3 Avalanche photodiodes

Backflashes have been shown to have a minor impact on the secure key rate and thus their existence is of relatively little concern to the QKD community. However,

their precise origin is still an open question. Further studies to explore this could be insightful, for example by measuring a very broad spectrum of the backflashes. This could help isolate whether they arise from the relaxation of hot carriers, which would produce broad emission, or recombination, which would be more correlated with the band gap of InP.

Currently, APDs used in QKD are almost exclusively manufactured to the SAGCM structure with an InGaAs absorption region and an InP multiplication. Whilst this has produced detection efficiencies as high as 55% [68], there is still room for improvement. A good area to focus would be the multiplication region as the aforementioned devices had quantum efficiencies as high as 69%, suggesting that improving the avalanche probability could raise the detection efficiency. InAlAs was shown to offer theoretically higher breakdown probabilities than InP [216], however devices manufactured with InAlAs multiplication regions have thus far had very large dark count rates making them impractical [84]. Another appealing approach is to use germanium as an absorption material as it is sensitive to wavelengths up to 1600 nm. Furthermore, it can be integrated with silicon (a candidate for the multiplication layer) and this would open the door for CMOS integrated electronics, allowing such devices to be fabricated easily, in large volumes and at low cost. This has been explored in several studies [217–219], most notably in a recent investigation [220] where single-photon detection efficiencies as high as 38% and lower afterpulsing rates than commercial InGaAs/InP devices were reported. Although lower temperatures were required to achieve reasonable dark count rates (78 K was need to go below a DCR of 10 kHz) and the gating frequency was limited to 1 kHz, this is an interesting avenue for the future of APDs in QKD.

7.3 Conclusion

Quantum key distribution (QKD) promises the ability for two parties to share a secret key with perfect, unbreakable security. However, this is only true in theory; in practice, components do not perform to their ideal best and show deviations from the theoretically predicted behaviour. These deviations can provide side-channels for Eve to exploit, although currently many of them are beyond current technology.

In recent years, as interest in quantum computing and secure communication has escalated, QKD has started to enter into real-world applications. Demonstrations over optical networks and using satellites have highlighted the growing activity surrounding quantum-secured communication and further underlined that this technology will likely play an ever-increasing role in everyday life. This means that significant effort is

required to make QKD practical and suitable for day-to-day use, as well as providing assurance that it can deliver the high level of security it promises. By writing standards and closing security loopholes, steps can be taken to achieve these goals.

Self-differencing avalanche photodiodes (SD APDs) are key enablers of QKD due to their ability to operate at room temperature, register high count rates and demonstrate excellent single-photon detection characteristics. It is therefore likely that SD APDs will be present in many QKD systems. Due to their potential for widespread use, it will become necessary to define standards to which these components will need to conform. A first step is to identify the best practice for their operation, which is performed in this thesis. By following a particular procedure, the users can have reasonable confidence that the APD has been setup appropriately. Inappropriate operation, in particular with regards to discrimination level, can allow Eve to perform a blinding attack which would otherwise be out of her reach. The use of a quenching resistor in the DC path to the APD also impacts the required optical power needed to achieve blinding.

Whilst following a certain prescription for operation of SD APDs was shown to be effective at preventing blinding, naturally these steps are not always carried out precisely. Ideally, the onus should be removed from the user, such that security is preserved even if human error is introduced. By placing an intensity modulator directly in front of the detector, and extinguishing a fraction of APD gates, the blinding attack can be effectively mitigated. Indeed, only an extinction ratio of 0.06 dB is required to ensure no blinding takes place, meaning the potential loss penalty would be small. A brief security analysis was carried out to demonstrate the effectiveness of this measure. It was also found that phase-encoded QKD protocols, which contain an asymmetric Mach-Zehnder interferometer at Bob, already possess this modulation due to the finite performance of the initial PBS. However, this is only applicable to continuous wave blinding; Eve can circumvent this using a pulsed laser and avoid interference at the final beamsplitter.

Blinding attacks have been demonstrated to be an effective technique available to Eve, but arguably a more powerful tool for her is the after-gate attack. This method of eavesdropping does not require a blinding laser, simply the trigger pulse, hence is theoretically more difficult to detect. This attack is demonstrated to be superficially effective at producing a quantum bit error rate (QBER) below the 11% threshold for key abortion, suggesting Eve could remain unnoticed. However, by incorporating delayed detection events into the analysis of the QBER, her presence can be revealed. These delayed detections arise due to a combination of effects: carriers failing to overcome the potential barrier formed at the interface between the InGaAs absorption and InP charge regions and carriers becoming trapped by defects in the InP multiplication

region. By assuming the material interface is the major contributor, we were able to bound the useable APD gating frequencies by Bob. This bound ensures the probability of delayed detection events is sufficiently low to perform QKD but also sufficiently high that they provide protection against the after-gate attack.

In the past, it has been shown that Eve can gain information passively without the need to interact with Bob's detectors at all. This can occur due to the emission of light by the APDs on detection, known as backflashes. The first study on GHz-gated APDs was performed with the use of superconducting nanowire single-photon detectors to monitor the backflashes. It was confirmed that faster gating frequencies, and therefore shorter gates and smaller avalanche charges, reduce the amount of backflashes. Eve's information was quantified and the subsequent impact on the secure key rate was determined and found to be negligible.

To sum up, QKD is moving ever closer to becoming a key component in a new era of security. APDs are are the most attractive candidate for use as single-photon detectors due to their ability to show excellent detection characteristics at temperatures close to room temperature as well as having a small footprint and low cost compared to their nearest competitors. By employing self-differencing circuitry, gated APDs have shown record detection efficiencies and secure key rates. Whilst some question marks have existed in the past over the practical security of these devices, this thesis has rigorously tackled the most prominent and dangerous of these, as well as showing that a significant amount of protection is already inherent within these detectors. This further highlights how self-differencing APDs are likely to play a major role in future QKD developments.

Bibliography

[1] X. Jiang, M. A. Itzler, R. Ben-Michael, and K. Slomkowski, "InGaAsP–InP Avalanche Photodiodes for Single Photon Detection," IEEE Journal of Selected Topics in Quantum Electronics, vol. 13, pp. 895–905, July 2007.

[2] D. Bouwmeester, A. K. Ekert, and A. Zeilinger, The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation. Springer Publishing Company, Incorporated, 1st ed., 2010.

[3] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," Transactions of the American Institute of Electrical Engineers, vol. XLV, pp. 295–301, Jan 1926.

[4] C. E. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal, vol. 28, pp. 656–715, Oct 1949.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, pp. 120–126, Feb. 1978.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, pp. 1484–1509, Oct. 1997.

[7] W. Knight, "IBM Raises the Bar with a 50-Qubit Quantum Computer." https://tinyurl.com/y34msyp6, 2017. Online; accessed 15-July-2019.

[8] J. Kelly, "A Preview of Bristlecone, Google's New Quantum Processor." https://tinyurl.com/y5sdasod, 2018. Online; accessed 15-July-2019.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984, pp. 175–179, 1984.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, pp. 145–195, Mar 2002.

[11] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, pp. 802–803, Oct. 1982.

[12] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," Journal of Cryptology, vol. 5, pp. 3–28, Jan 1992.

[13] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s Quantum Key Distribution," J. Lightwave Technol., vol. 36, pp. 3427–3433, Aug 2018.

[14] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure Quantum Key Distribution over 421 km of Optical Fiber," Phys. Rev. Lett., vol. 121, p. 190502, Nov 2018.

[15] Bunandar, Darius and Lentine, Anthony and Lee, Catherine and Cai, Hong and Long, Christopher M. and Boynton, Nicholas and Martinez, Nicholas and DeRose, Christopher and Chen, Changchen and Grein, Matthew and Trotter, Douglas and Starbuck, Andrew and Pomerene, Andrew and Hamilton, Scott and Wong, Franco N. C. and Camacho, Ryan and Davids, Paul and Urayama, Junji and Englund, Dirk, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X, vol. 8, p. 021009, Apr 2018.

[16] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," Opt. Express, vol. 23, pp. 33437–33447, Dec 2015.

[17] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photonics, vol. 9, pp. 163–168, 2015.

[18] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, "Modulator-Free Coherent-One-Way Quantum Key Distribution," Laser & Photonics Reviews, vol. 11, no. 4, p. 1700067, 2017.

[19] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express, vol. 21, pp. 24550–24565, Oct 2013.

[20] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A, vol. 68, p. 022317, Aug 2003.

[21] K. Inoue and Y. Iwai, "Differential-quadrature-phase-shift quantum key distribution," Phys. Rev. A, vol. 79, p. 022319, Feb 2009.

[22] S. Kawakami, T. Sasaki, and M. Koashi, "Security of the differential-quadrature-phase-shift quantum key distribution," Phys. Rev. A, vol. 94, p. 022332, Aug 2016.

[23] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. Yuan, and A. J. Shields, "Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution," Applied Physics Letters, vol. 111, no. 26, p. 261106, 2017.

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, pp. 1301–1350, Sep 2009.

[25] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120 km using ultra high purity single-photon source and superconducting single-photon detectors," Scientific Reports, vol. 5, p. 14383, 2015.

[26] M. Fox, Quantum Optics: An Introduction. Oxford Univeristy Press, 2006.

[27] Y. Hu, X. Peng, T. Li, and H. Guo, "On the Poisson approximation to photon distribution for faint lasers," Physics Letters A, vol. 367, no. 3, pp. 173 – 176, 2007.

[28] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," Phys. Rev. A, vol. 51, pp. 1863–1869, Mar 1995.

[29] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," New Journal of Physics, 2002.

[30] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett., vol. 91, p. 057901, Aug 2003.

[31] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett., vol. 94, p. 230504, Jun 2005.

[32] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett., vol. 92, p. 057901, Feb 2004.

[33] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt., vol. 48, no. 13, pp. 2023–2038, 2001.

[34] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," Phys. Rev. X, vol. 5, p. 031030, Sep 2015.

[35] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, no. 13, p. 130503, 2012.

[36] S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," Phys. Rev. Lett., vol. 108, p. 130502, Mar 2012.

[37] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," Physical Review Letters, vol. 59, no. 18, p. 2044, 1987.

[38] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks," Physical Review Letters, vol. 111, Sept. 2013.

[39] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nature Photonics, vol. 10, pp. 312–315, Apr. 2016.

[40] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw, J. A. Stern, S. W. Nam, D. Oblak, Q. Zhou, J. A. Slater, and W. Tittel, "Measurement-device-independent quantum key distribution: from idea towards application," Journal of Modern Optics, vol. 62, no. 14, pp. 1141–1150, 2015.

[41] C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden, "Detector-device-independent quantum key distribution," Applied Physics Letters, vol. 105, no. 22, 2014.

[42] Z. Cao, Q. Zhao, and X. Ma, "Performance of device-independent quantum key distribution," Physical Review A, vol. 94, July 2016.

[43] B. Qi, "Trustworthiness of detectors in quantum key distribution with untrusted detectors," Physical Review A, vol. 91, Feb. 2015.

[44] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, "Insecurity of detector-device-independent quantum key distribution," Phys. Rev. Lett., vol. 117, p. 250505, Dec 2016.

[45] M. Lucamarini, Z. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, pp. 400–403, 2018.

[46] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nature Communications, vol. 8, 2017.

[47] M. Minder, M. Pittaluga, G. L. Robert, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," Nature Photonics, vol. 13, pp. 334–338, 2018.

[48] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," Phys. Rev. Lett., vol. 123, p. 100506, Sep 2019.

[49] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," Phys. Rev. X, vol. 9, p. 021046, Jun 2019.

[50] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," Phys. Rev. Lett., vol. 123, p. 100505, Sep 2019.

[51] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," Phys. Rev. A, vol. 98, p. 062323, Dec 2018.

[52] X.-Y. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, "Asymmetric sending or not sending twin-field quantum key distribution in practice," Phys. Rev. A, vol. 99, p. 062316, Jun 2019.

[53] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," Phys. Rev. Applied, vol. 11, p. 034053, Mar 2019.

[54] M. Tomammichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nature Communications, vol. 3, p. 634, 2012.

[55] S.-C. Zhao, X.-H. Han, Y. Xiao, Y. Shen, Y.-J. Gu, and W.-D. Li, "Performance of underwater quantum key distribution with polarization encoding," J. Opt. Soc. Am. A, vol. 36, pp. 883–892, May 2019.

[56] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," Appl. Opt., vol. 58, pp. 3902–3907, May 2019.

[57] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. w. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," Opt. Express, vol. 26, pp. 22563–22573, Aug 2018.

[58] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature, vol. 549, pp. 43–47, Sept. 2017.

[59] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, M. Li, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," Physical Review Letters, vol. 119, Nov. 2017.

[60] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett., vol. 120, p. 030501, Jan 2018.

[61] T. Miya, Y. Terunuma, T. Hosaka, and T. Miyashita, "Ultimate low-loss single-mode fibre at 1.55 μm," Electronics Letters, vol. 15, pp. 106–108, Feb 1979.

[62] L. Lydersen, V. Makarov, and J. Skaar, "Secure gated detection scheme for quantum cryptography," Phys. Rev. A, vol. 83, p. 032306, Mar 2011.

[63] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express, vol. 26, pp. 6010–6020, Mar 2018.

[64] J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J. P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Information, vol. 5, p. 101, Dec. 2019.

[65] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New Journal of Physics, vol. 11, no. 7, p. 075001, 2009.

[66] T. Vogl, R. Lecamwasam, B. C. Buchler, Y. Lu, and P. K. Lam, "Compact Cavity-Enhanced Single-Photon Generation with Hexagonal Boron Nitride," ACS Photonics, vol. 6, pp. 1955–1962, Aug. 2019.

[67] T. Vogl, R. Lecamwasam, B. C. Buchler, Y. Lu, and P. K. Lam, "Supplementary Information: Compact cavity-enhanced single-photon generation with hexagonal boron nitride," p. 8.

[68] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," J. Appl. Phys., vol. 117, p. 083109, feb 2015.

[69] J. Münzberg, A. Vetter, F. Beutel, W. Hartmann, S. Ferrari, W. H. P. Pernice, and C. Rockstuhl, "Superconducting nanowire single-photon detector implemented in a 2d photonic crystal cavity," Optica, vol. 5, pp. 658–665, May 2018.

[70] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," Applied Physics Letters, vol. 104, p. 081108, Feb. 2014.

[71] W.-H. Jiang, X.-J. Gao, Y.-Q. Fang, J.-H. Liu, Y. Zhou, L.-Q. Jiang, W. Chen, G. Jin, J. Zhang, and J.-W. Pan, "Miniaturized high-frequency sine wave gating InGaAs/InP single-photon detector," Review of Scientific Instruments, vol. 89, no. 12, p. 123104, 2018.

[72] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nature Photonics, vol. 7, pp. 210–214, 2013.

[73] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," Opt. Express, vol. 16, pp. 3032–3040, Mar 2008.

[74] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett., vol. 117, p. 190501, Nov 2016.

[75] "sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,"

[76] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, Oct. 2019.

[77] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express, vol. 19, pp. 10387–10409, May 2011.

[78] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express, vol. 22, pp. 21739–21756, Sep 2014.

[79] Y. Yang, "China trial paves way for 'unhackable' communications network," Jul 2017.

[80] R. Alléaume, I. P. Degiovanni, A. Mink, T. E. Chapuran, N. Lütkenhaus, M. Peev, C. J. Chunnilall, V. Martin, M. Lucamarini, M. Ward, and A. Shields, "Worldwide standardization activity for quantum key distribution," in 2014 IEEE Globecom Workshops (GC Wkshps), pp. 656–661, Dec 2014.

[81] K. Nishida, K. Taguchi, and Y. Matsumoto, "InGaAsP heterostructure avalanche photodiodes with high avalanche gain," Applied Physics Letters, vol. 35, no. 3, pp. 251–253, 1979.

[82] S. R. Forrest, M. DiDomenico, R. G. Smith, and H. J. Stocker, "Evidence for tunneling in reverse-biased III-V photodetector diodes," Applied Physics Letters, vol. 36, no. 7, p. 580, 1980.

[83] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," Light: Science & Applications, vol. 4, p. e286, May 2015.

[84] X. Meng, C. H. Tan, S. Dimler, J. P. R. David, and J. S. Ng, "1550 nm InGaAs/InAlAs single photon avalanche diode at room temperature," Optics Express, vol. 22, p. 22608, Sept. 2014.

[85] X. Meng, S. Xie, X. Zhou, N. Calandri, M. Sanzaro, A. Tosi, C. H. Tan, and J. S. Ng, "InGaAs/InAlAs single photon avalanche diode for 1550 nm photons," Royal Society Open Science, vol. 3, p. 150584, Mar. 2016.

[86] Y. Kang, P. Mages, A. Clawson, P. Yu, M. Bitter, Z. Pan, A. Pauchard, S. Hummel, and Y. Lo, "Fused InGaAs-Si avalanche photodiodes with low-noise performances," IEEE Photonics Technology Letters, vol. 14, pp. 1593–1595, Nov. 2002.

[87] J. Campbell, S. Demiguel, F. Ma, A. Beck, X. Guo, S. Wang, X. Zheng, X. Li, J. Beck, M. Kinch, A. Huntington, L. Coldren, J. Decobert, and N. Tscherptner, "Recent Advances in Avalanche Photodiodes," IEEE Journal of Selected Topics in Quantum Electronics, vol. 10, pp. 777–787, July 2004.

[88] R. J. McIntyre, "Multiplication noise in uniform avalanche diodes," IEEE Transactions on Electron Devices, no. 1, pp. 164–168, 1966.

[89] C. A. Armiento, S. H. Groves, and C. E. Hurwitz, "Ionization coefficients of electrons and holes in InP," Applied Physics Letters, vol. 35, no. 4, pp. 333–335, 1979.

[90] I. Umebu, A. N. M. M. Choudhury, and P. N. Robson, "Ionization coefficients measured in abrupt InP junctions," Applied Physics Letters, vol. 36, no. 4, pp. 302–303, 1980.

[91] J. C. Campbell, A. G. Dentai, W. S. Holden, and B. L. Kasper, "High-performance avalanche photodiode with separate absorption 'grading' and multiplication regions," Electronics Letters, vol. 19, pp. 818–820, September 1983.

[92] Y. Matsushima, K. Sakai, and Y. Noda, "New type InGaAs/InP heterostructure avalanche photodiode with buffer layer," IEEE Electron Device Letters, vol. 2, pp. 179–181, July 1981.

[93] P. A. Hiskett, G. S. Buller, A. Y. Loudon, J. M. Smith, I. Gontijo, A. C. Walker, P. D. Townsend, and M. J. Robertson, "Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55 μm," Appl. Opt., vol. 39, pp. 6818–6829, Dec 2000.

[94] C. L. F. Ma, M. J. Deen, and L. E. Tarof, "Multiplication in separate absorption, grading, charge, and multiplication InP-InGaAs avalanche photodiodes," IEEE Journal of Quantum Electronics, vol. 31, pp. 2078–2089, Nov 1995.

[95] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," Appl. Phys. Lett., vol. 104, no. 2, p. 021101, 2014.

[96] M. Moshkova, A. Divochiy, P. Morozov, Y. Vakhtomin, A. Antipov, P. Zolotov, V. Seleznev, M. Ahmetov, and K. Smirnov, "High-performance superconducting photon-number-resolving detectors with 86% system efficiency at telecom range," J. Opt. Soc. Am. B, vol. 36, pp. B20–B25, Mar 2019.

[97] A. Divochiy, M. Misiaszek, Y. Vakhtomin, P. Morozov, K. Smirnov, P. Zolotov, and P. Kolenderski, "Single photon detection system for visible and infrared spectrum range," Opt. Lett., vol. 43, pp. 6085–6088, Dec 2018.

[98] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett., vol. 98, p. 010503, Jan 2007.

[99] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," Nat. Photon., vol. 3, pp. 696–705, 2009.

[100] G. S. Buller and R. J. Collins, "Single-photon generation and detection," Measurement Science and Technology, vol. 21, no. 1, 2010.

[101] M. A. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova, "Advances in InGaAsP-based avalanche diode single photon detectors," Journal of Modern Optics, vol. 58, pp. 174–200, Feb. 2011.

[102] J. P. Donnelly, E. K. Duerr, K. A. Mcintosh, E. A. Dauler, D. C. Oakley, S. H. Groves, C. J. Vineis, L. J. Mahoney, K. M. Molvar, P. I. Hopman, K. E. Jensen, G. M. Smith, S. Verghese, and D. C. Shaver, "Design considerations for 1.06- μm InGaAsP-InP Geiger-Mode Avalanche Photodiodes," IEEE Journal of Quantum Electronics, vol. 42, pp. 797–809, Aug 2006.

[103] N. Calandri, M. Sanzaro, A. Tosi, and F. Zappa, "Charge Persistence in InGaAs/InP Single-Photon Avalanche Diodes," IEEE Journal of Quantum Electronics, vol. 52, pp. 1–7, Mar. 2016.

[104] M. Liu, C. Hu, X. Bai, X. Guo, J. C. Campbell, Z. Pan, and M. M. Tashima, "High-Performance InGaAs/InP Single-Photon Avalanche Photodiode," IEEE Journal of Selected Topics in Quantum Electronics, vol. 13, pp. 887–894, July 2007.

[105] X. Jiang, M. A. Itzler, R. Ben-Michael, K. Slomkowski, M. A. Krainak, S. Wu, and X. Sun, "Afterpulsing Effects in Free-Running InGaAsP Single-Photon Avalanche Diodes," IEEE Journal of Quantum Electronics, vol. 44, pp. 3–11, Jan 2008.

[106] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X, vol. 2, p. 041010, Nov 2012.

[107] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," Appl. Opt., vol. 35, pp. 1956–1976, Apr 1996.

[108] A. Lacaita and M. Mastrapasqua, "Strong dependence of time resolution on detector diameter in single photon avalanche diodes," Electronics Letters, vol. 26, pp. 2053–2054, Nov 1990.

[109] A. Gaidash, V. Egorov, and A. Gleim, "Revealing beam-splitting attack in a quantum cryptography system with a photon-number-resolving detector," J. Opt. Soc. Am. B, vol. 33, pp. 1451–1455, Jul 2016.

[110] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," Reviews of Modern Physics, vol. 79, pp. 135–174, Jan. 2007.

[111] O. Thomas, Z. Yuan, and A. Shields, "Practical photon number detection with electric field-modulated silicon avalanche photodiodes," Nature Communications, vol. 3, p. 644, Jan. 2012.

[112] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection," Applied Physics Letters, vol. 107, p. 071106, Aug. 2015.

[113] Y. Tamura, Y. Suzuki, T. Fujita, T. Kurabayashi, T. Baba, K. Makino, S. Nakamura, and K. Yamamoto, "Development of InGaAs MPPC for NIR photon counting applications," in Proc. SPIE 10528, Optical Components and Materials XV, 105280Z, 2018.

[114] X. Chen, E. Wu, L. Xu, Y. Liang, G. Wu, and H. Zeng, "Photon-number resolving performance of the InGaAs/InP avalanche photodiode with short gates," Applied Physics Letters, vol. 95, no. 13, p. 131118, 2009.

[115] B. E. Kardynal, Z. L. Yuan, and A. J. Shields, "An avalanche photodiode-based photon-number-resolving detector," Nature Photonics, vol. 2, pp. 425–428, jul 2008.

[116] G. Wu, Y. Jian, E. Wu, and H. Zeng, "Photon-number-resolving detection based on InGaAs/InP avalanche photodiode in the sub-saturated mode," Opt. Express, vol. 17, pp. 18782–18787, Oct 2009.

[117] D. Bronzi, F. Villa, S. Tisa, A. Tosi, and F. Zappa, "SPAD Figures of Merit for Photon-Counting, Photon-Timing, and Imaging Applications: A Review," IEEE Sensors Journal, vol. 16, pp. 3–12, Jan 2016.

[118] J. C. Campbell, "Recent advances in telecommunications avalanche photodiodes," Journal of Lightwave Technology, vol. 25, pp. 109–121, Jan 2007.

[119] A. Tosi, N. Calandri, M. Sanzaro, and F. Acerbi, "Low-Noise, Low-Jitter, High Detection Efficiency InGaAs/InP Single-Photon Avalanche Diode," IEEE Journal of Selected Topics in Quantum Electronics, vol. 20, pp. 192–197, Nov 2014.

[120] A. Gallivanoni, I. Rech, and M. Ghioni, "Progress in Quenching Circuits for Single Photon Avalanche Diodes," IEEE Transactions on Nuclear Science, Dec. 2010.

[121] T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. A. Itzler, and H. Zbinden, "Free-running single-photon detection based on a negative feedback InGaAs APD," Journal of Modern Optics, vol. 59, no. 17, pp. 1481–1488, 2012.

[122] S. Cova, A. Longoni, and G. Ripamonti, "Active-quenching and gating circuits for single-photon avalanche diodes," IEEE Transactions on Nuclear Science, vol. 29, pp. 599–601, Feb 1982.

[123] F. Zappa, M. Ghioni, S. Cova, C. Samori, and A. C. Giudice, "An integrated active-quenching circuit for single-photon avalanche diodes," IEEE Transactions on Instrumentation and Measurement, vol. 49, pp. 1167–1175, Dec 2000.

[124] M. Stipčević, B. G. Christensen, P. G. Kwiat, and D. J. Gauthier, "Advanced active quenching circuit for ultra-fast quantum cryptography," Opt. Express, vol. 25, pp. 21861–21876, Sep 2017.

[125] G. Ribordy, N. Gisin, O. Guinnard, D. Stuck, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: Current performance," Journal of Modern Optics, vol. 51, no. 9-10, pp. 1381–1398, 2004.

[126] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, "2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," in Proc. SPIE 7681, Advanced Photon Counting Techniques IV, 76810Z, 2010.

[127] B. Korzh, T. Lunghi, K. Kuzmenko, G. Boso, and H. Zbinden, "Afterpulsing studies of low-noise InGaAs/InP single-photon negative-feedback avalanche diodes," Journal of Modern Optics, vol. 62, no. 14, pp. 1151–1157, 2015.

[128] N. Namekata, S. Adachi, and S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," Opt. Express, vol. 17, pp. 6275–6282, Apr 2009.

[129] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," Opt. Express, vol. 19, pp. 10632–10639, May 2011.

[130] D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, Y.-J. Qian, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Sine-wave gating InGaAs/InP single photon detector with ultralow afterpulse," Applied Physics Letters, vol. 110, no. 11, p. 111104, 2017.

[131] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett., vol. 91, no. 4, p. 04114, 2007.

[132] K. A. Patel, J. F. Dynes, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Gigacount/second photon detection with InGaAs avalanche photodiodes," Electron. Lett., vol. 48, no. 2, pp. 111–113, 2012.

[133] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt., vol. 52, no. 5, pp. 691–705, 2005.

[134] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nature Communications, vol. 2, p. 349, jun 2011.

[135] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, "Homodyne-detector-blinding attack in continuous-variable quantum key distribution," Phys. Rev. A, vol. 98, p. 012312, Jul 2018.

[136] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," New Journal of Physics, vol. 13, no. 11, p. 113042, 2011.

[137] L. Lydersen, N. Jain, C. Wittmann, O. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "Superlinear threshold detectors in quantum cryptography," Phys. Rev. A, vol. 84, p. 032320, Sep 2011.

[138] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," Opt. Express, vol. 26, pp. 21020–21032, Aug 2018.

[139] N. Zhou, W.-H. Jiang, L.-K. Chen, Y.-Q. Fang, Z.-D. Li, H. Liang, Y.-A. Chen, J. Zhang, and J.-W. Pan, "Sine wave gating silicon single-photon detectors for multiphoton entanglement experiments," Review of Scientific Instruments, vol. 88, no. 8, p. 083102, 2017.

[140] V. Makarov, "Controlling passively quenched single photon detectors by bright light," New J. Phys., vol. 11, no. 6, p. 065003, 2009.

[141] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photon., vol. 4, pp. 686–689, oct 2010.

[142] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, "Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption," IEEE J. Quant. Electron., vol. 52, pp. 1–11, Nov 2016.

[143] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A, vol. 74, p. 022313, Aug 2006.

[144] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A, vol. 78, p. 042333, Oct 2008.

[145] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device Calibration Impacts Security of Quantum Key Distribution," Phys. Rev. Lett., vol. 107, p. 110501, Sep 2011.

[146] Y.-Y. Fei, X.-D. Meng, M. Gau, H. Wang, and Z. Ma, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," Scientific Reports, vol. 8, p. 4283, 2018.

[147] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, M. Koashi, and A. Tomita, "Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses," npj Quantum Information, vol. 4, 2018.

[148] J. P. Salvestrini, L. Guilbert, M. Fontana, M. Abarkan, and S. Gille, "Analysis and Control of the DC Drift in $LiNbO_3$-Based Mach–Zehnder Modulators," Journal of Lightwave Technology, vol. 29, pp. 1522–1534, May 2011.

[149] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, "Quantum key distribution with distinguishable decoy states," Phys. Rev. A, vol. 98, p. 012330, Jul 2018.

[150] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution," Opt. Lett., vol. 43, pp. 5110–5113, Oct 2018.

[151] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multi-wavelength sources," Phys. Rev. A, vol. 84, p. 062308, Dec 2011.

[152] L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," Journal of Modern Optics, vol. 58, no. 8, pp. 680–685, 2011.

[153] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett., vol. 89, p. 037902, Jun 2002.

[154] H. Takesue, S. Woo Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors," Nature Photonics, vol. 1, pp. 343–348, 2007.

[155] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Applied Physics Letters, vol. 87, no. 19, p. 194108, 2005.

[156] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express, vol. 18, pp. 27938–27954, Dec 2010.

[157] C. Groves, R. Ghin, J. David, and G. Rees, "Temperature dependence of impact ionization in GaAs," IEEE Transactions on Electron Devices, vol. 50, pp. 2027–2031, Oct. 2003.

[158] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, "Laser Damage Helps the Eavesdropper in Quantum Cryptography," Physical Review Letters, vol. 112, Feb. 2014.

[159] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, "Creation of backdoors in quantum communications via laser damage," Phys. Rev. A, vol. 94, p. 030302, Sep 2016.

[160] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD," Nat. Photon., vol. 4, no. 12, pp. 800–801, 2010.

[161] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography," Appl. Phys. Lett., vol. 98, no. 23, p. 231104, 2011.

[162] M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, "Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems," Phys. Rev. A, vol. 88, p. 062335, 2013.

[163] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," Appl. Phys. Lett., vol. 93, p. 031109, 2008.

[164] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," Contemporary Physics, vol. 57, pp. 366–387, 2016.

[165] R. E. Warburton, M. Itzler, and G. S. Buller, "Free-running, room temperature operation of an InGaAs/InP single-photon avalanche diode," Appl. Phys. Lett., vol. 94, p. 071116, 2009.

[166] T. Lee and S. Sze, "Depletion layer capacitance of cyclindrical and spherical p-n junctions," Solid-State Electronics, vol. 10, pp. 1105 – 1108, 1967.

[167] N. Namekata, S. Sasamori, and S. Inoue, "800 MHz Single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," Opt. Express, vol. 14, pp. 10043–10049, Oct 2006.

[168] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes," Applied Physics Letters, vol. 95, no. 9, p. 091103, 2009.

[169] Y. Nambu, S. Takahashi, K. Yoshino, A. Tanaka, M. Fujiwara, M. Sasaki, A. Tajima, S. Yorozu, and A. Tomita, "Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution," Opt. Express, vol. 19, pp. 20531–20541, Oct 2011.

[170] Y. Liang, E. Wu, X. Chen, M. Ren, Y. Jian, G. Wu, and H. Zeng, "Low-Timing-Jitter Single-Photon Detection Using 1-GHz Sinusoidally Gated InGaAs/InP Avalanche Photodiode," IEEE Photonics Technology Letters, vol. 23, pp. 887–889, July 2011.

[171] A. Restelli, J. C. Bienfang, and A. L. Migdall, "Single-photon detection efficiency up to 50% at 1310nm with an InGaAs/InP avalanche diode gated at 1.25GHz," Applied Physics Letters, vol. 102, no. 14, p. 141104, 2013.

[172] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems," Opt. Express, vol. 20, pp. 18911–18924, 2012.

[173] Ø. Marøy, V. Makarov, and J. Skaar, "Secure detection in quantum key distribution by real-time calibration of receiver," Quantum Science and Technology, vol. 2, p. 044013, sep 2017.

[174] M. S. Lee, B. K. Park, M. K. Woo, C. H. Park, Y.-S. Kim, S.-W. Han, and S. Moon, "Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme," Phys. Rev. A, vol. 94, p. 062321, Dec 2016.

[175] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A, vol. 73, p. 022320, Feb 2006.

[176] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New J. Phys., vol. 4, no. 1, p. 41, 2002.

[177] L. Lydersen, V. Makarov, and J. Skaar, "Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]," Applied Physics Letters, vol. 99, no. 19, p. 196101, 2011.

[178] L. Lydersen, C. Wiechers, C. Wittman, D. Elsr, J. Skaar, and V. Makarov, "Avoiding the blinding attack in QKD," Nature Photonics, vol. 4, no. 801, 2010.

[179] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Response to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'" [Appl. Phys. Lett. 99, 196101 (2011)]," Applied Physics Letters, vol. 99, no. 19, p. 196102, 2011.

[180] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Random Variation of Detector Efficiency: A Countermeasure Against Detector Blinding Attacks for Quantum Key Distribution," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, pp. 192–196, May 2015.

[181] K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, "Inherent security of phase coding quantum key distribution systems against detector blinding attacks," Laser Physics Letters, vol. 15, no. 9, p. 095203, 2018.

[182] A. Fedorov, I. Gerhardt, A. Huang, J. Jogenfors, Y. Kurochkin, A. Lamas-Linares, J. Åke Larsson, G. Leuchs, L. Lydersen, V. Makarov, and J. Skaar, "Comment on 'Inherent security of phase coding quantum key distribution systems against detector blinding attacks' (2018 Laser Phys. Lett . 15 095203)," Laser Physics Letters, vol. 16, no. 1, p. 019401, 2019.

[183] K. A. Balygin, A. N. Klimov, I. B. Bobrov, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, "Response to Comment on 'Inherent security of phase coding quantum key distribution systems against detector blinding attacks'," Laser Physics Letters, vol. 16, no. 1, p. 019402, 2019.

[184] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution," Phys. Rev. Applied, vol. 9, p. 044027, Apr 2018.

[185] M. Bass, "Handbook of Optics: Volume II; Devices, Measurements, and Properties; Second Edition," The Handbook of Photonics: Second Edition. Edited by Michael Bass and Eric W. Van Stryland and David R. Williams and William L. Wolfe. ISBN 0-07-047974-7. Published by R. R. Donnelly Sons Company, 1995.

[186] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," New Journal of Physics, vol. 13, p. 013043, Jan 2011.

[187] M. Koashi, "Efficient quantum key distribution with practical sources and detectors," arXiv preprint arXiv:quant-ph/0609180, 2006.

[188] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "Quantum key distribution with hacking countermeasures and long term field trial," Sci. Rep., vol. 7, no. 1, p. 1978, 2017.

[189] M. Ren, X. Gu, Y. Liang, W. Kong, E. Wu, G. Wu, and H. Zeng, "Laser ranging at 1550 nm with 1-GHz sine-wave gated InGaAs/InP APD single-photon detector," Opt. Express, vol. 19, pp. 13497–13502, Jul 2011.

[190] Y. Nambu, S. Takahashi, K. Yoshino, A. Tanaka, M. Fujiwara, M. Sasaki, A. Tajima, S. Yorozu, and A. Tomita, "Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution," Opt. Express, vol. 19, no. 21, pp. 20531–20541, 2011.

[191] Y. Liang, E. Wu, X. Chen, M. Ren, Y. Jian, G. Wu, and H. Zeng, "Low-timing-jitter single-photon detection using 1-GHz sinusoidally gated InGaAs/InP avalanche photodiode," IEEE Photon. Technol. Lett., vol. 23, no. 13, p. 887, 2011.

[192] N. Walenta, T. Lunghi, O. Guinnard, R. Houlmann, H. Zbinden, and N. Gisin, "Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature," J. Appl. Phys., vol. 112, no. 6, p. 063106, 2012.

[193] S. R. Forrest, O. K. Kim, and R. G. Smith, "Optical response time of $In_{0.53}Ga_{0.47}As$/InP avalanche photodiodes," Applied Physics Letters, vol. 41, no. 1, pp. 95–98, 1982.

[194] F. Zappa, A. Lacaita, S. Cova, and P. Webb, "Nanosecond single-photon timing with InGaAs/InP photodiodes," Opt. Lett., vol. 19, pp. 846–848, Jun 1994.

[195] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors," Phys. Rev. Applied, vol. 10, p. 064062, Dec 2018.

[196] S. Pellegrini, R. E. Warburton, L. J. J. Tan, J. S. Ng, A. B. Krysa, K. Groom, J. P. R. David, S. Cova, M. J. Robertson, and G. S. Buller, "Design and performance of an InGaAs-InP single-photon avalanche diode detector," IEEE Journal of Quantum Electronics, vol. 42, pp. 397–403, April 2006.

[197] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. R. Roberts, A. W. Sharpe, S. J. Savory, Z. Yuan, and A. J. Shields, "Setting best-practice criteria for self-differencing avalanche photodiodes in quantum key distribution," in Proc. SPIE 10442, Quantum Information Science and Technology III, 104420L, 2017.

[198] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Applied Physics Letters, vol. 92, no. 20, p. 201104, 2008.

[199] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," Phys. Rev. X, vol. 2, p. 041010, Nov 2012.

[200] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Opt. Express, vol. 16, no. 23, pp. 18790–18979, 2008.

[201] R. Newman, "Visible light from a silicon $p-n$ junction," Phys. Rev., vol. 100, pp. 700–703, Oct 1955.

[202] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?," Journal of Modern Optics, vol. 48, no. 13, pp. 2039–2047, 2001.

[203] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," Light: Science and Applications, vol. 6, no. e16261, 2017.

[204] H. Finkelstein, M. Gross, Y. Lo, and S. Esener, "Analysis of hot-carrier luminescence for infrared single-photon upconversion and readout," IEEE Journal of Selected Topics in Quantum Electronics, vol. 13, pp. 959–966, July 2007.

[205] P. Klocek, "Handbook of infrared optical materials," Handbook of infrared optical materials. Edited by Paul Klocek. ISBN 0-8247-8468-5. Published by Marcel DEKKER, Inc., 1991.

[206] L. Marini, R. Camphausen, B. J. Eggleton, and S. Palomba, "Deterministic filtering of breakdown flashing at telecom wavelengths," Applied Physics Letters, vol. 111, no. 21, p. 213501, 2017.

[207] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer, "Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes," Opt. Express, vol. 25, pp. 30388–30394, Nov 2017.

[208] R. D. Younger, K. A. McIntosh, J. W. Chludzinski, D. C. Oakley, L. J. Mahoney, J. E. Funk, J. P. Donnelly, and S. Verghese, "Crosstalk Analysis of Integrated Geiger-mode Avalanche Photodiode Focal Plane Arrays," in Proc. SPIE 7320, Advanced Photon Counting Techniques III, 73200Q, 2009.

[209] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices," Quantum Info. Comput., vol. 4, pp. 325–360, sep 2004.

[210] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," The European Physical Journal D, vol. 41, p. 599, Jan 2007.

[211] A. Duplinskiy and D. Sych, "Bounding light source side channels in QKD via Hong-Ou-Mandel interference," arXiv preprint arXiv:1908.04703, 2019.

[212] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, "Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch," Phys. Rev. A, vol. 100, p. 022325, Aug 2019.

[213] T. Ferreira da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Safeguarding quantum key distribution through detection randomization," IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, pp. 159–167, May 2015.

[214] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nature Communications, vol. 8, p. 13984, 2017.

[215] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," npj Quantum Information, vol. 5, 2019.

[216] S. C. Liew Tat Mun, C. H. Tan, S. J. Dimler, L. J. J. Tan, J. S. Ng, Y. L. Goh, and J. P. R. David, "A Theoretical Comparison of the Breakdown Behavior of $In_{0.52}Al_{0.48}As$ and InP Near-Infrared Single-Photon Avalanche Photodiodes," IEEE Journal of Quantum Electronics, vol. 45, pp. 566–571, May 2009.

[217] N. J. D. Martinez, C. T. Derose, R. W. Brock, A. L. Starbuck, A. T. Pomerene, A. L. Lentine, D. C. Trotter, and P. S. Davids, "High performance waveguide-coupled Ge-on-Si linear mode avalanche photodiodes," Opt. Express, vol. 24, pp. 19072–19081, Aug 2016.

[218] N. J. D. Martinez, M. Gehl, C. T. Derose, A. L. Starbuck, A. T. Pomerene, A. L. Lentine, D. C. Trotter, and P. S. Davids, "Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode," Opt. Express, vol. 25, pp. 16130–16139, Jul 2017.

[219] R. E. Warburton, G. Intermite, M. Myronov, P. Allred, D. R. Leadley, K. Gallacher, D. J. Paul, N. J. Pilgrim, L. J. M. Lever, Z. Ikonic, R. W. Kelsall, E. Huante-Cerón, A. P. Knights, and G. S. Buller, "Ge-on-Si Single-Photon Avalanche Diode Detectors: Design, Modeling, Fabrication, and Characterization at Wavelengths 1310 and 1550 nm," IEEE Transactions on Electron Devices, vol. 60, pp. 3807–3813, Nov 2013.

[220] P. Vines, K. Kuzmenko, J. Kirdoda, D. C. S. Dumas, M. M. Mirza, R. W. Millar, D. J. Paul, and G. S. Buller, "High performance planar germanium-on-silicon single-photon avalanche diode detectors," Nature Communications, vol. 10, 2019.